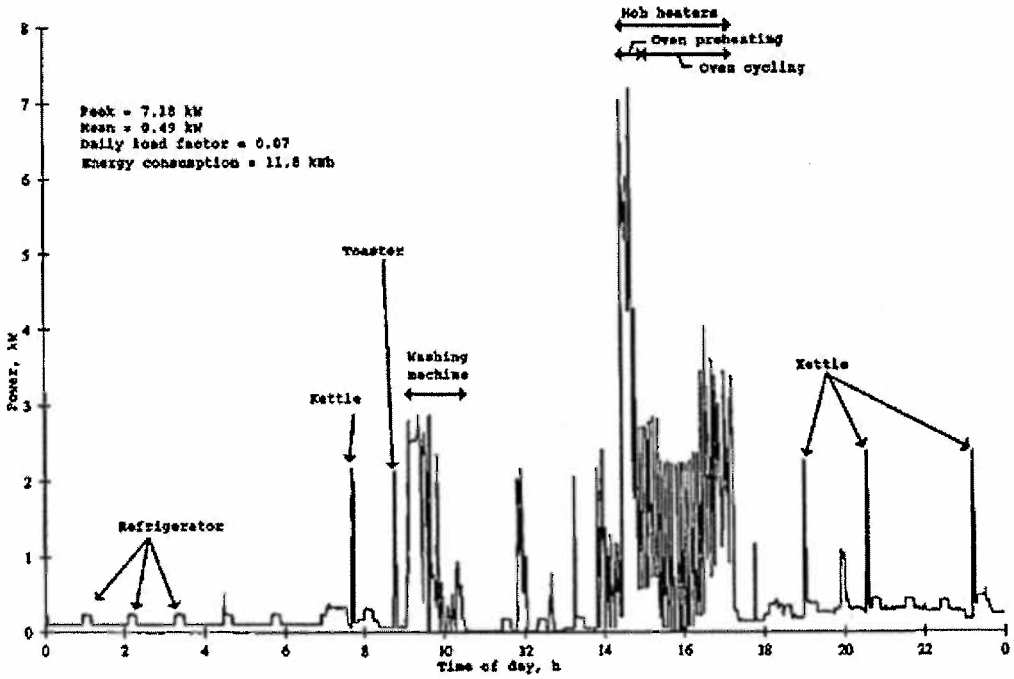
DECEMBER 2, 2014 STATEMENT BY DR. JAMES KRESS



This illustration details personal usage of electrical appliances in one home constructed from the analysis of electrical consumption data collected over a 24-hour period.

In their zeal to collect their $83,828,878 part of the $3,425,718,323 from the Federal Recovery Act: Smart Grid Investment Grants, DTE has inflicted an unprecedented level of intrusion, command and control over their customers and their use of electricity, which enables utilities, government and any hacker who takes an interest, surveillance and control of personal behavior at unprecedented levels. DTE has abused "customers" and invaded and destroyed property. DTE has run roughshod over customers' legitimate concerns regarding privacy, property destruction and abuse.

The DTE "SmartCurrents" program includes three projects: deploy a large-scale network of 660,000 surveillance devices (aka "smart meters"), implement dynamic pricing to 5,000 customers and smart appliances to 300 customers. The surveillance capabilities of these so-called "smart meters" is clearly documented in the February 3, 2012 "Smart Meter Data: Privacy and Cybersecurity" report published by the Congressional Research Service.

These surveillance devices continuously measure and record your use of electricity. When picked up by DTE, this information can then be automatically analyzed by complex computer programs to extract what household activities are being performed and when they occur.

For example, shown above is an illustration of the detailed personal usage of electrical appliances in one home constructed from the analysis of electrical consumption data collected over a 24 hour period.

As you can see, these surveillance devices can be used to determine when your refrigerator cycles, when you wash your clothes, when you cook your food – anything in your home that is done using electricity can be monitored. The result: highly detailed information about your personal activities carried on within the four walls of the home is captured by DTE – the fundamental definition of surveillance.

In addition, activities that might be revealed through analysis of home appliance use data include personal sleep and work habits, cooking and eating schedules, the presence of certain medical equipment and other specialized devices, presence or absence of persons in the home, and activities that might seem to signal illegal, or simply unorthodox,

behavior. As a result, information collected by the Smart Grid becomes highly valuable for many purposes other than energy efficiency, most prominently: commercial exploitation by advertisers and marketers, household surveillance by law enforcement, and access by criminals attempting to break into homes or commit identity theft (reference both "Joint Comments Of The Center For Democracy & Technology And The Electronic Frontier Foundation On Proposed Policies And Findings Pertaining To The Smart Grid" and "New "Smart Meters" for Energy Use Put Privacy at Risk - The Electronic Frontier Foundation")

DTE has also seemed to "forget" about one "minor item" — every surveillance device installation is a violation of Michigan Penal Code, Act 328 of 1931, MCL 750.539d which makes it a felony to install a device for the purpose of observing, recording, transmitting, photographing or eavesdropping in a "Private Place".

The MCL 750.539d Sec. 539d. specifically states (in part):

(1) A person shall not do either of the following:

(a) Install, place, or use in any private place, without the consent of the person or persons entitled to privacy in that place, any device for observing, recording, transmitting, photographing, or eavesdropping upon the sounds or events in that place.

(b) Distribute, disseminate, or transmit for access by any other person a recording, photograph, or visual image the person knows or has reason to know was obtained in violation of this section.

(3) A person who violates or attempts to violate this section is guilty of a crime as follows:

For a violation or attempted violation: the person is guilty of a felony punishable by imprisonment for not more than 2 years or a fine of not more than $2,000.00, or both. If the person was previously convicted of violating or attempting to violate this section (and/or subsection (1)(b), the person is guilty of a felony punishable by imprisonment for not more than 5 years or a fine of not more than $5,000.00, or both.

The Attorney General must respond to complaints filed against DTE's clear violation of 750.539d Sec. 539d. The functionaries of government should be held accountable for their failure to enforce the law. DTE should be forced to stop its criminal activity, remove existing surveillance devices and be criminally charged with multiple counts of violation of MCL 750.539d Sec. 539d.

If you value your Liberty and independence from government control of the minutia of your lives, you should immediately contact your legislative representatives, the Attorney General, the MPSC and the governor and demand this felonious activity be halted, reversed, and prosecuted — immediately.

Dr. James Kress is a resident of Salem Township (Washtenaw County) and is a member of the Institute of Electrical and Electronic Engineers, The American Institute of Physics, The American Chemical Society, The American Association for Cancer Research, and the American Society of Clinical Oncologists. He has a PhD in Physical Chemistry from The University of Notre Dame with over 30 years of experience in Research, Development, Production and Management in Chemical Engineering, Physics, Electronic Device design and production, Systems Engineering, Information Technology and BioTechnology development and application.

Dr. Kress is currently President of The KressWorks Foundation, a Michigan Non-profit, 501c3 organization dedicated to providing Systems Engineering Solutions to diseases such as Cancer.

Attachments:

Smart Meter Data: Privacy and Cybersecurity – Congressional Research Service

Joint Comments Of The Center For Democracy & Technology And The Electronic Frontier Foundation On Proposed Policies And Findings Pertaining To The Smart Grid

New "Smart Meters" for Energy Use Put Privacy at Risk - The Electronic Frontier Foundation

Smart Meter Data: Privacy and Cybersecurity

Brandon J. Murrill
Legislative Attorney

Edward C. Liu
Legislative Attorney

Richard M. Thompson II
Legislative Attorney

February 3, 2012

Congressional Research Service
7-5700
www.crs.gov
R42338

Summary

Fueled by stimulus funding in the American Recovery and Reinvestment Act of 2009 (ARRA), electric utilities have accelerated their deployment of smart meters to millions of homes across the United States with help from the Department of Energy's Smart Grid Investment Grant program. As the meters multiply, so do issues concerning the privacy and security of the data collected by the new technology. This Advanced Metering Infrastructure (AMI) promises to increase energy efficiency, bolster electric power grid reliability, and facilitate demand response, among other benefits. However, to fulfill these ends, smart meters must record near-real time data on consumer electricity usage and transmit the data to utilities over great distances via communications networks that serve the smart grid. Detailed electricity usage data offers a window into the lives of people inside of a home by revealing what individual appliances they are using, and the transmission of the data potentially subjects this information to interception or theft by unauthorized third parties or hackers.

Unforeseen consequences under federal law may result from the installation of smart meters and the communications technologies that accompany them. This report examines federal privacy and cybersecurity laws that may apply to consumer data collected by residential smart meters. It begins with an examination of the constitutional provisions in the Fourth Amendment that may apply to the data. As we progress into the 21st century, access to personal data, including information generated from smart meters, is a new frontier for police investigations. The Fourth Amendment generally requires police to have probable cause to search an area in which a person has a reasonable expectation of privacy. However, courts have used the third-party doctrine to deny protection to information a customer gives to a business as part of their commercial relationship. This rule is used by police to access bank records, telephone records, and traditional utility records. Nevertheless, there are several core differences between smart meters and the general third-party cases that may cause concerns about its application. These include concerns expressed by the courts and Congress about the ability of technology to potentially erode individuals' privacy.

If smart meter data and transmissions fall outside of the protection of the Fourth Amendment, they may still be protected from unauthorized disclosure or access under the Stored Communications Act (SCA), the Computer Fraud and Abuse Act (CFAA), and the Electronic Communications Privacy Act (ECPA). These statutes, however, would appear to permit law enforcement to access smart meter data for investigative purposes under procedures provided in the SCA, ECPA, and the Foreign Intelligence Surveillance Act (FISA), subject to certain conditions. Additionally, an electric utility's privacy and security practices with regard to consumer data may be subject to Section 5 of the Federal Trade Commission Act (FTC Act). The Federal Trade Commission (FTC) has recently focused its consumer protection enforcement on entities that violate their privacy policies or fail to protect data from unauthorized access. This authority could apply to electric utilities in possession of smart meter data, provided that the FTC has statutory jurisdiction over them. General federal privacy safeguards provided under the Federal Privacy Act of 1974 (FPA) protect smart meter data maintained by federal agencies, including data held by federally owned electric utilities.

A companion report from CRS focusing on policy issues associated with smart grid cybersecurity, CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by Richard J. Campbell, is also available.

Contents

Overview 1
Smart Meter Data: Privacy and Security Concerns 3
Detailed Information on Household Activities 3
Increased Potential for Theft or Breach of Data 6
Smart Meters and the Fourth Amendment 7
State Action: Privately Versus Publicly Owned Utilities 8
Privately Owned and Operated Utilities 8
Publicly Owned and Operated Utilities 10
Reasonable Expectation of Privacy in Smart Meter Data 13
Third-Party Doctrine 14
Privacy in the Home 16
Mosaic and Dragnet Theories 19
Assumption of the Risk—Consent 21
Statutory Protection of Smart Meter Data 22
The Electronic Communications Privacy Act (ECPA) 23
The Stored Communications Act (SCA) 24
Electronic Communication Services 25
Remote Computing Services 27
The Computer Fraud and Abuse Act (CFAA) 28
The Federal Trade Commission Act (FTC Act) 29
Covered Electric Utilities 29
Investor-Owned Utilities 30
Publicly Owned Utilities 30
Federally Owned Utilities 34
Cooperatively Owned Utilities 35
Enforcement of Data Privacy and Security 40
"Deceptive" Privacy Statements 40
"Unfair" Failure to Secure Consumer Data 41
Penalties 42
The Federal Privacy Act of 1974 (FPA) 43
Federally Owned Utilities as "Agencies" 43
Smart Meter Data as a Protected "Record" 44
Requirements 44

Figures

Figure 1. Identification of Household Activities from Electricity Usage Data 5

Contacts

Author Contact Information 45

Overview

Smart meter technology is a key component of the Advanced Metering Infrastructure (AMI)[1] that will help the smart grid[2] link the "two-way flow of electricity with the two-way flow of information."[3] Privacy and security concerns surrounding smart meter technology arise from the meters' essential functions, which include (1) recording near-real time data on consumer electricity usage; (2) transmitting this data to the smart grid using a variety of communications technologies;[4] and (3) receiving communications from the smart grid, such as real-time energy prices or remote commands that can alter a consumer's electricity usage to facilitate demand response.[5]

Beneficial uses of AMI are developing rapidly, and like the early Internet, many applications remain unforeseen.[6] At a basic level, smart meters will permit utilities to "collect, measure, and analyze energy consumption data for grid management, outage notification, and billing purposes."[7] The meters may increase energy efficiency by giving consumers greater control over their use of electricity,[8] as well as permitting better integration of plug-in electric vehicles and renewable energy sources.[9] They may also aid in the development of a more reliable electricity grid that is better equipped to withstand cyber attacks and natural disasters, and help to decrease peak demand for electricity.[10] To be useful for these purposes, and many others, data recorded by

---

[1] AMI includes the meters at the consumer's residence or business, the communications networks that send data between the consumer and utility, and the data management systems that store and process data for the utility. ELECTRIC POWER RESEARCH INST., ADVANCED METERING INFRASTRUCTURE (AMI) (2007), *available at* http://www.ferc.gov/eventcalendar/Files/20070423091846-EPRI%20-%20Advanced%20Metering.pdf. The primary function of AMI is to "combine interval data measurement with continuously available remote communications" to increase energy efficiency and grid reliability, and decrease expenses borne by the utility and consumer. *Id.*

[2] The Energy Independence and Security Act of 2007 (EISA) lists ten characteristics of a smart grid. These include "[i]ncreased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid"; "[d]evelopment and incorporation of demand response, demand-side resources, and energy-efficiency resources"; and "[d]eployment of "smart" technologies (real-time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation." EISA, P.L. 110-140, §1301, 121 Stat. 1492, 1783-84 (2007) (to be codified at 42 U.S.C. §17381).

[3] DEP'T OF ENERGY, COMMUNICATIONS REQUIREMENTS OF SMART GRID TECHNOLOGIES 1 (2010) [hereinafter DEP'T OF ENERGY COMMUNICATIONS REPORT], *available at* http://energy.gov/sites/prod/files/gcprod/documents/Smart_Grid_Communications_Requirements_Report_10-05-2010.pdf.

[4] *Id.* at 3, 5. These technologies include fiber optics, wireless networks, satellite, and broadband over power line. *Id.*

[5] *Id.* at 20. "Demand response is the reduction of the consumption of electric energy by customers in response to an increase in the price of electricity or heavy burdens on the system." *Id.*

[6] DEP'T OF ENERGY, DATA ACCESS AND PRIVACY ISSUES RELATED TO SMART GRID TECHNOLOGIES 5, 9 (2010) [hereinafter DEP'T OF ENERGY PRIVACY REPORT], *available at* http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf; *see also* ELIAS LEAKE QUINN, SMART METERING & PRIVACY: EXISTING LAW AND COMPETING POLICIES: A REPORT FOR THE COLORADO PUBLIC UTILITIES COMMISSION 1, 12 (2009) [hereinafter COLORADO PRIVACY REPORT], *available at* http://www.dora.state.co.us/puc/docketsdecisions/DocketFilings/091-593EG/091-593EG_Spring2009Report-SmartGridPrivacy.pdf.

[7] DEP'T OF ENERGY COMMUNICATIONS REPORT, *supra* note 3, at 12.

[8] Companies are developing several new applications that use smart meter data to offer consumers and utilities better control over energy usage, for example by determining the energy efficiency of specific appliances within the household. DEP'T OF ENERGY PRIVACY REPORT, *supra* note 6, at 5, 9; *see also* COLORADO PRIVACY REPORT, *supra* note 6, at 1, 12.

[9] DEP'T OF ENERGY COMMUNICATIONS REPORT, *supra* note 3, at 1.

[10] *Id.* at 3.

smart meters must be highly detailed, and, consequently, it may show what individual appliances a consumer is using.[11] The data must also be transmitted to electric utilities—and possibly to third parties outside of the smart grid—subjecting it to potential interception or theft as it travels over communications networks and is stored in a variety of physical locations.[12]

These characteristics of smart meter data present privacy and security concerns that are likely to become more prevalent as government-backed initiatives expand deployment of the meters to millions of homes across the country. In the American Recovery and Reinvestment Act of 2009 (ARRA), Congress appropriated funds for the implementation of the Smart Grid Investment Grant (SGIG) program administered by the Department of Energy.[13] This program now permits the federal government to reimburse up to 50% of eligible smart grid investments, which include the cost to electric utilities of buying and installing smart meters.[14] In its annual report on smart meter deployment, the Federal Energy Regulatory Commission cited statistics showing that the SGIG program has helped fund the deployment of about 7.2 million meters as of September 2011.[15] At completion, the program will have partially funded the installation of 15.5 million meters.[16] By 2015, the Institute for Electric Efficiency expects that a total of 65 million smart meters will be in operation throughout the United States.[17]

Installation of smart meters and the communications technologies that accompany them may have unforeseen legal consequences for those who generate, seek, or use the data recorded by the meters. These consequences may arise under existing federal laws or constitutional provisions governing the privacy of electronic communications, data retention, computer misuse, foreign surveillance, and consumer protection. This report examines federal privacy and cybersecurity laws that may apply to consumer data collected by residential smart meters. It examines the legal implications of smart meter technology for consumers who generate the data, law enforcement officers who seek smart meter data from utilities, utilities that store the data, and hackers who access smart grid technology to steal consumer data or interfere with it. This report looks at federal laws that may pertain to the data when it is (1) stored in a utility-owned smart meter at a consumer's residence; (2) in transit between the meter and the smart grid by way of various communications technologies; and (3) stored on computers in the grid. This report does not address state or local laws, such as regulations by state Public Utilities Commissions, that may establish additional responsibilities for some electric utilities with regard to smart meter data. It also does not discuss the mandatory cybersecurity and reliability standards enforced by the North

[11] *See* NAT'L INST. OF STANDARDS AND TECH., GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 2, PRIVACY AND THE SMART GRID 14 (2010) [hereinafter NIST PRIVACY REPORT], *available at* http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.

[12] *Id.* at 3-4, 23-24, 29.

[13] The act provides $4.5 billion for "electricity delivery and energy reliability," which includes "activities to modernize the electric grid, to include demand responsive equipment," as well as "programs authorized under title XIII of the Energy Independence and Security Act of 2007." ARRA, P.L. 111-5, 123 Stat. 115, 138-39.

[14] ARRA §405(5), (8), 123 Stat. 115, 143-44 (amendment to be codified at 42 U.S.C. §17386) (amending the Energy Independence and Security Act of 2007 (EISA) to allow for the reimbursement of up to 50% of qualifying smart grid investments instead of only 20%); *see also* EISA, P.L. 110-140, §1306, 121 Stat. 1492, 1789-91 (to be codified as amended at 42 U.S.C. §17386) (initially establishing the SGIG program).

[15] FED. ENERGY REGULATORY COMM'N, ASSESSMENT OF DEMAND RESPONSE & ADVANCED METERING 3 (2011), *available at* http://www.ferc.gov/legal/staff-reports/11-07-11-demand-response.pdf.

[16] *Id.*

[17] INST. FOR ELECTRIC EFFICIENCY, UTILITY-SCALE SMART METER DEPLOYMENTS, PLANS & PROPOSALS 1 (2011), *available at* http://www.edisonfoundation.net/iee/issuebriefs/SmartMeter_Rollouts_0911.pdf.

American Electric Reliability Corporation, which impose obligations on utilities that participate in the generation or transmission of electricity.[18]

General federal privacy safeguards provided under the Federal Privacy Act of 1974 (FPA) protect smart meter data maintained by federal agencies, including data held by federally owned electric utilities. Section 5 of the Federal Trade Commission Act (FTC Act) allows the Federal Trade Commission (FTC) to bring enforcement proceedings against electric utilities that violate their privacy policies or fail to protect meter data from unauthorized access, provided that the FTC has statutory jurisdiction over the utilities.

It is unclear how Fourth Amendment protection from unreasonable search and seizures would apply to smart meter data, due to the lack of cases on this issue. However, depending upon the manner in which smart meter services are presented to consumers, smart meter data may be protected from unauthorized disclosure or unauthorized access under the Stored Communications Act (SCA), the Computer Fraud and Abuse Act (CFAA), and the Electronic Communications Privacy Act (ECPA). If smart meter data is protected by these statutes, law enforcement would still appear to have the ability to access it for investigative purposes under procedures provided in the SCA, ECPA, and the Foreign Intelligence Surveillance Act (FISA).

Smart Meter Data: Privacy and Security Concerns

Residential smart meters present privacy and cybersecurity issues[19] that are likely to evolve with the technology.[20] In 2010, the National Institute of Standards and Technology (NIST) published a report identifying some of these issues, which fall into two main categories: (1) privacy concerns that smart meters will reveal the activities of people inside of a home by measuring their electricity usage frequently over time;[21] and (2) fears that inadequate cybersecurity measures surrounding the digital transmission of smart meter data will expose it to misuse by authorized and unauthorized users of the data.[22]

Detailed Information on Household Activities

Smart meters offer a significantly more detailed illustration of a consumer's energy usage than regular meters. Traditional meters display data on a consumer's *total* electricity usage and are typically read manually once per month.[23] In contrast, smart meters can provide *near real-time* usage data by measuring usage electronically at a much greater frequency, such as once every 15

[18] For additional information on the development of mandatory national smart grid privacy and cybersecurity standards by federal agencies, see MASS. INST. OF TECH., THE FUTURE OF THE ELECTRIC GRID 197-234 (2011) [hereinafter MIT GRID STUDY]; *see also* CRS Report R41886, *The Smart Grid and Cybersecurity—Regulatory Policy and Issues*, by Richard J. Campbell.

[19] According to the authors of the MIT study, cybersecurity "refers to all the approaches taken to protect data, systems, and networks from deliberate attack as well as accidental compromise, ranging from preparedness to recovery." MIT GRID STUDY, *supra* note 18, at 208. Closely related is the concept of "information privacy," which "deals with policy issues ranging from identification and collection to storage, access, and use of information." *Id.* at 219 n.viii.

[20] *See* NIST PRIVACY REPORT, *supra* note 11, at 1.

[21] *Id.* at 4, 11. Data that offers a high degree of detail is said to be "granular." *Id.*

[22] *See id.* at 4, 23-24, 29.

[23] *Id.* at 2, 9.

minutes.[24] Current smart meter technology allows utilities to measure usage as frequently as once every minute.[25] By examining smart meter data, it is possible to identify which appliances a consumer is using and at what times of the day, because each type of appliance generates a unique electric load "signature."[26] NIST wrote in 2010 that "research shows that analyzing 15-minute interval aggregate household energy consumption data can by itself pinpoint the use of most major home appliances."[27] A report for the Colorado Public Utilities Commission discussed an Italian study that used "artificial neural networks" to identify individual "heavy-load appliance uses" with 90% accuracy using 15-minute interval data from a smart meter.[28] Similarly, software-based algorithms would likely allow a person to extract the unique signatures of individual appliances from meter data that has been collected less frequently and is therefore less detailed.[29]

By combining appliance usage patterns, an observer could discern the behavior of occupants in a home over a period of time.[30] For example, the data could show whether a residence is occupied, how many people live in it, and whether it is "occupied by more people than usual."[31] According to the Department of Energy, smart meters may be able to reveal occupants' "daily schedules (including times when they are at or away from home or asleep), whether their homes are equipped with alarm systems, whether they own expensive electronic equipment such as plasma TVs, and whether they use certain types of medical equipment."[32] **Figure 1**, which appears in NIST's report on smart grid cybersecurity, shows how smart meter data could be used to decipher the activities of a home's occupants by matching data on their electricity usage with known appliance load signatures.

[24] *Id.* at 13.

[25] COLORADO PRIVACY REPORT, *supra* note 6, at 2. Some utilities may elect to receive data at less frequent intervals because "backhauling real-time or near real-time data from the billions of devices that may eventually be connected to the Smart Grid would require not only tremendous bandwidth" but also greater data storage capacities that could make the effort "economically infeasible." DEP'T OF ENERGY COMMUNICATIONS REPORT, *supra* note 3, at 20. However, the "trend" is for utilities to collect data more frequently. *See* COLORADO PRIVACY REPORT, *supra* note 6, at A-1 n.111.

[26] NIST PRIVACY REPORT, *supra* note 11, at 2, 14.

[27] *Id.* at 14. *But see* DEP'T OF ENERGY PRIVACY REPORT, *supra* note 6, at 9 (claiming, in 2010, that smart meter technology "cannot yet identify individual appliances and devices in the home in detail, but this will certainly be within the capabilities of subsequent generations of Smart Grid technologies").

[28] COLORADO PRIVACY REPORT, *supra* note 6, at 3 n.7, A-8.

[29] *Id.* at A-9.

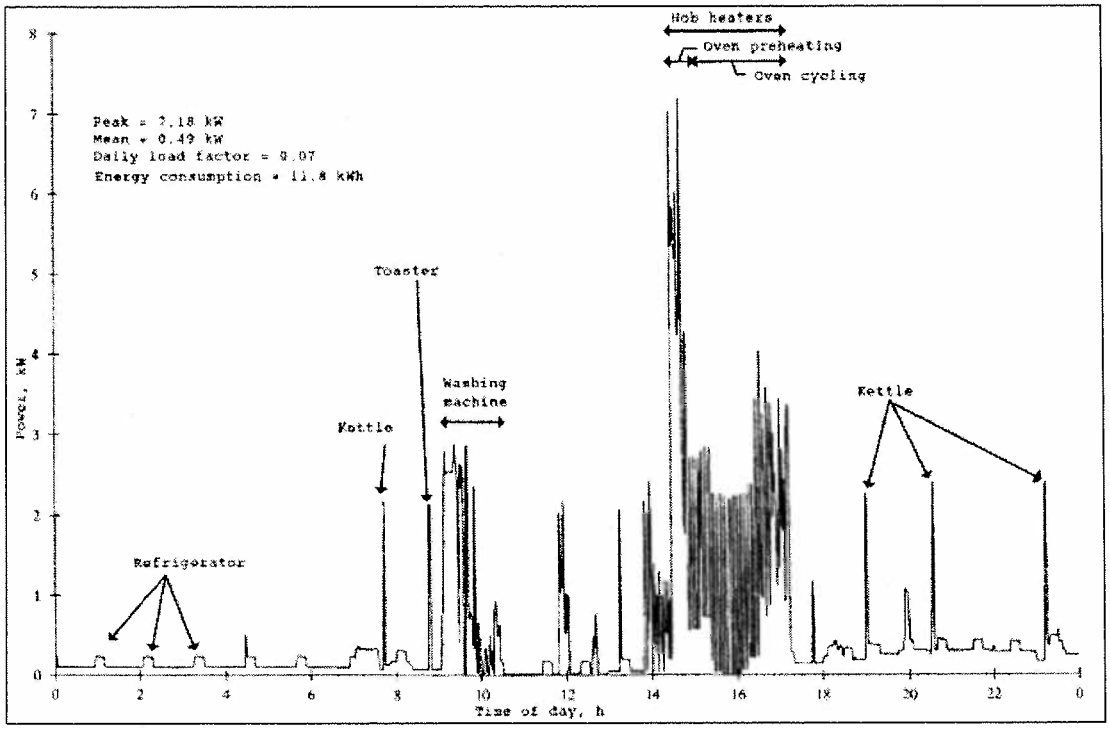
[30] NIST PRIVACY REPORT, *supra* note 11, at 6 & n.9.

[31] *Id.* at 11.

[32] DEP'T OF ENERGY PRIVACY REPORT, *supra* note 6, at 2.

Figure 1. Identification of Household Activities from Electricity Usage Data

Unique Electric Load Signatures of Common Household Appliances



Source: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 2, PRIVACY AND THE SMART GRID 13 (2010), *available at* http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.

Note: Researchers constructed this picture from electricity usage data collected at one-minute intervals using a nonintrusive appliance load monitoring (NALM) device, which is similar to a smart meter in the way that it records usage data. For a comparison of the technologies, see COLORADO PRIVACY REPORT, *supra* note 6, at A-1 to A-9.

Smart meter data that reveals which appliances a consumer is using has potential value for third parties, including the government. In the past, law enforcement agents have examined *monthly* electricity usage data from *traditional* meters in investigations of people they suspected of illegally growing marijuana.[33] For example, in *United States v. Kyllo*, a federal agent subpoenaed the suspect's electricity usage records from the utility and "compared the records to a spreadsheet for estimating average electrical use and concluded that Kyllo's electrical usage was abnormally high, indicating a possible indoor marijuana grow operation."[34] If law enforcement officers obtained near-real time data on a consumer's electricity usage from the utility company, their ability to monitor household activities would be amplified significantly.[35] For example, by observing when occupants use the most electricity, it may be possible to discern their daily schedules.[36]

[33] NIST PRIVACY REPORT, *supra* note 11, at 11, 29; *see also* United States v. Kyllo, 190 F.3d 1041, 1043 (9th Cir. 1999), *rev'd on other grounds*, 533 U.S. 27 (2001).

[34] *Kyllo*, 190 F.3d at 1043.

[35] *See supra* notes 26-32 and accompanying text.

[36] *See supra* note 32 and accompanying text.

As smart meter technology develops and usage data grows more detailed, it could also become more valuable to private third parties outside of the grid.[37] Data that reveals which appliances a person is using could permit health insurance companies to determine whether a household uses certain medical devices, and appliance manufacturers to establish whether a warranty has been violated.[38] Marketers could use it to make targeted advertisements.[39] Criminals could use it to time a burglary and figure out which appliances they would like to steal.[40] If a consumer owned a plug-in electric vehicle, data about where the vehicle has been charged could permit someone to identify a person's location and travel history.[41]

Even privacy safeguards, such as "anonymizing" data so that it does not reflect identity, are not foolproof.[42] By comparing anonymous data with information available in the public domain, it is sometimes possible to identify an individual—or, in the context of smart meter data, a particular household.[43] Moreover, a smart grid will collect more than just electricity usage data. It will also store data on the account holder's name, service address, billing information, networked appliances in the home, and meter IP address, among other information.[44] Many smart meters will also provide transactional records as they send data to the grid, which would show the time that the meter transmitted the data and the location or identity of the transmitter.[45]

Increased Potential for Theft or Breach of Data

Smart grid technology relies heavily on two-way communication to increase energy efficiency and reliability, including communication between smart meters and the utility (or other entity) that stores data for the grid.[46] Many different technologies will transmit data to the grid, including "traditional twisted-copper phone lines, cable lines, fiber optic cable, cellular, satellite, microwave, WiMAX, power line carrier, and broadband over power line."[47] Of these communications platforms, wireless technologies are likely to play a "prominent role" because they present fewer safety concerns and cost less to implement than wireline technologies.[48] According to the Department of Energy, a typical utility network has four "tiers" that collect and transmit data from the consumer to the utility.[49] These include "(1) the core backbone—the primary path to the utility data center; (2) backhaul distribution—the aggregation point for

[37] NIST PRIVACY REPORT, *supra* note 11, at 14, 35-36.

[38] *Id.* at 27-28.

[39] *Id.* at 28.

[40] *Id.* at 31.

[41] *Id.*

[42] *Id.* at 13.

[43] *See id.* at 13, 25.

[44] *Id.* at 26-27.

[45] *Id.* at 12 (drawing a comparison to telecommunications providers' "call detail records").

[46] *Id.* at 3; DEP'T OF ENERGY COMMUNICATIONS REPORT, *supra* note 3, at 3 (stating that "integrated two-way communications ... allows for dynamic monitoring of electricity use as well as the potential for automated electricity use scheduling."). As more consumers become generators of electricity through the use of "fuel cells, wind turbines, solar roofs, and the like," the importance of two-way communication will increase. MIT GRID STUDY, *supra* note 18, at 201.

[47] DEP'T OF ENERGY COMMUNICATIONS REPORT, *supra* note 3, at 3.

[48] *Id.* at 5, 51 n.215.

[49] *Id.* at 16.

neighborhood data; (3) the access point—typically the smart meter; and, (4) the HAN—the home network."[50] Energy usage data moves from the smart meter,[51] and then to an "aggregation point" outside of the residence such as "a substation, a utility pole-mounted device, or a communications tower."[52] The aggregation points gather data from multiple meters and "backhaul" it to the utility using fiber, T1, microwave, or wireless technology.[53] Utilities typically rely on their own private networks to communicate with smart meters because they have found these networks to be more reliable and less expensive than commercial networks.[54]

As NIST explains, consumer data moving through a smart grid becomes stored in many locations both within the grid and within the physical world.[55] Thus, because it is widely dispersed, it becomes more vulnerable to interception by unauthorized parties[56] and to accidental breach.[57] The movement of data also increases the potential for it to be stolen by unauthorized third parties while it is in transit, particularly when it travels over a wireless network[58]—or through communications components that may be incompatible with one another or possess outdated security protections.[59]

Smart Meters and the Fourth Amendment

The use of smart meters presents the recurring conflict between law enforcement's need to effectively investigate and combat crime and our desire for privacy while in our homes. With smart meters, police will have access to data that might be used to track residents' daily lives and routines while in their homes, including their eating, sleeping, and showering habits, what appliances they use and when, and whether they prefer the television to the treadmill, among a host of other details.[60] Though a potential boon to police, access to this data is not limitless. The Fourth Amendment, which establishes the constitutional parameters for government investigations, may restrict access to smart meter data or establish rules by which it can be obtained.[61] The Fourth Amendment ensures that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...."[62] This section discusses whether the collection and use of smart meter data may

---

[50] *Id.*

[51] The home network will be used to provide *consumers* with near real-time data on their energy usage. *Id.* at 13-15.

[52] *Id.* Many urban installations use wireless mesh networks to carry data from the meters to the aggregation point. These networks are more reliable because each smart meter can serve as a router in the network, providing redundant network coverage. *Id.* at 18.

[53] *Id.* at 16, 19.

[54] *Id.* at 4, 19, 44.

[55] NIST PRIVACY REPORT, *supra* note 11, at 23.

[56] *Id.* at 23-24.

[57] *Id.* at 29.

[58] *See id.* at 9, 12, 33, and 36.

[59] MIT GRID STUDY, *supra* note 18, at 209, 213-16.

[60] Jack I. Lerner & Deirdre K. Mulligan, *Taking the "Long View" on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3, ¶ 3 (2008).

[61] Additionally, as described below, there are federal statutory protections that may pertain to this data. State constitutional and statutory safeguards may also apply, but these are beyond the scope of this report.

[62] U.S. CONST. amend IV.

contravene this protection. Although there is no Fourth Amendment case on point, analogous cases may provide guidance.[63]

To assess whether there has been a Fourth Amendment violation, two primary questions must be asked: (1) whether there was state action; that is, was there sufficient government involvement in the alleged wrongdoing to trigger the Fourth Amendment; and (2) whether the person had an expectation of privacy that society is prepared to deem reasonable.[64] If the first question is answered in the affirmative, then the analysis moves to the second question. But if no state action is found, the analysis ends there and the Fourth Amendment does not apply. This subpart will first determine whether access to smart meter data by police, or by privately and publicly owned utilities, satisfies the state action doctrine, thereby warranting further Fourth Amendment review.

State Action: Privately Versus Publicly Owned Utilities

Most of the safeguards for civil liberties and individual rights contained in the U.S. Constitution apply only to actions by state and federal governments.[65] This rule, known as the state action doctrine, arises when a victim claims his constitutional rights have been violated, and therefore must prove the wrongdoer had sufficient connections with the government to warrant a remedy.[66] Applying the state action test is intended to determine whether a utility's collection and dissemination of smart meter data is governed by the Fourth Amendment, and if so, to what extent. Although there are many variations in the governance and ownership of utilities—some are privately owned, others publicly owned, some federally operated, and still others nonprofit cooperatives—they generally fall into two broad categories: public and private.[67] This section will analyze the constitutional differences between privately and publicly owned utilities under the state action doctrine and a public records theory.

Privately Owned and Operated Utilities

It is broadly said that the Fourth Amendment applies only to acts by the government.[68] But there are at least two exceptions to this rule. First, if a utility performs a function traditionally exercised by the government, it may be considered a state actor under the public function exception. Second, the Fourth Amendment may apply when a private utility acts as an instrument or agent of the police.[69]

---

[63] For additional analyses of smart meters under the Fourth Amendment, see Cheryl Dancey Balough, *Privacy Implications of Smart Meters*, 86 CHI.-KENT L. REV. 161 (2011); *see also* QUINN, *supra* note 6, at 28 ("[I]nterval data of electricity consumption appears to be in something of a no-man's-land under Supreme Court Fourth Amendment jurisprudence.").

[64] California v. Ciraolo, 476 U.S. 207, 211 (1986) (citing Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).

[65] Civil Rights Cases, 109 U.S. 3, 11 (1883) ("It is State action of a particular character that is prohibited. Individual invasion of individual rights is not the subject-matter of the [Fourteenth] amendment."); *see* JOHN E. NOWAK & RONALD D. ROTUNDA, CONSTITUTIONAL LAW §12.1(a)(i) (8th ed. 2010).

[66] NOWAK & ROTUNDA, *supra* note 65.

[67] Determining whether a private actor is sufficiently "public" is not clear-cut. Then Justice Rehnquist noted, "[t]he true nature of the State's involvement may not be immediately obvious, and detailed inquiry may be required in order to determine whether the test is met." Jackson v. Metropolitan Edison Co., 419 U.S. 345, 351 (1974).

[68] Burdeau v. McDowell, 256 U.S. 465, 475 (1921).

[69] *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

Under the public function exception, a nominally private entity is treated as a state actor when it assumes a role traditionally played by the government.[70] Determining when this exception applies has not proved easy,[71] but it is reasonably clear that private utilities do not, in most instances, satisfy it. In *Jackson v. Metropolitan Edison Co.*, a customer sued a privately owned utility under the Civil Rights Act of 1871 for improperly shutting off her service without providing her notice or a hearing.[72] The Supreme Court asked whether there was a close enough nexus between the state and the utility for the acts of the latter to be treated as those of the former.[73] Although the utility was heavily regulated by the state, it was held not to be a state actor.[74] The Court reasoned that the provision of utility service is not generally an "exclusive prerogative of the State."[75] Also absent was the symbiotic relationship between the utility and the state found in previous cases.[76] Though its holding was broad, the Court did not foreclose the possibility that a privately owned utility could be a state actor under different circumstances.[77] This possibility, however, appears narrow.

The Fourth Amendment may also apply to a private utility if its acts were directed by the government. Generally, searches performed by private actors without police participation or encouragement are not governed by the Fourth Amendment.[78] A search by a private insurance investigator, for instance, was not a "search" in the constitutional sense, though the evidence was ultimately used by the government at trial.[79] This result differs, however, if there is sufficient government involvement. If the search has been ordered or requested by the government, the private actor will become an "instrument or agent of the state" and must abide by Fourth Amendment strictures.[80] For example, the Fourth Amendment does not apply when a telephone company installs a pen register on its own initiative.[81] The same action constitutes a search, however, if requested by the government.[82]

This theory applies not only to direct instigation, but also on a broad, programmatic level. In the 1960s and 1970s the federal government required privately owned and operated airlines to institute new security measures to combat airline hijacking.[83] In *United States v. Davis*, the airline

---

[70] Marsh v. Alabama, 326 U.S. 501 (1946) (holding that privately owned property was equivalent to "community shopping center" thus private party was subject to the First and Fourteenth Amendments).

[71] *See* NOWAK & ROTUNDA, *supra* note 65, §12.2.

[72] *Jackson*, 419 U.S. at 347; *see also* Mays v. Buckeye Rural Elec. Coop., Inc., 277 F.3d 873, 880-81 (6th Cir. 2002) (holding that nonprofit cooperative utility was not a state actor under the federal constitution); Spickler v. Lee, No. 02-1954, 2003 U.S. App. LEXIS 6227, at *2 (1st Cir. March 31, 2003) (holding that private electric utility company was not a state actor).

[73] *Jackson*, 419 U.S. at 351.

[74] *Id.* at 358-59.

[75] *Id.* at 353.

[76] *Id.* at 357.

[77] *Id.* at 351.

[78] 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE §1.8, at 255 (4th ed. 2004).

[79] United States v. Howard, 752 F.2d 220, 227-28 (6th Cir. 1985).

[80] Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971) (internal quotation marks omitted); *see* LAFAVE, *supra* note 78, §1.8(b).

[81] United States v. Manning, 542 F.2d 685, 686 (6th Cir. 1976).

[82] People of Dearborn Heights v. Hayes, 82 Mich. App. 253, 258 (1978).

[83] United States v. Davis, 482 F.2d 893, 897-903 (9th Cir. 1973).

searched a passenger based on these requirements and found a loaded gun.[84] The Ninth Circuit held that it made no difference whether the search was conducted by a private or public official: "the search was part of the overall, nation-wide anti-hijacking effort, and constituted 'state action' for purposes of the Fourth Amendment."[85] Thus, if a private party is required to perform a search or collect data under federal or state laws or regulations, there will be sufficient state action for the Fourth Amendment to apply. Or, put another way, the government cannot circumvent the Fourth Amendment by requiring a private party to initiate a search or implement an investigative program.

This agency theory might apply to the collection of smart meter data. If the utility is accessing this information "independent of the government's intent to collect evidence for use in a criminal prosecution,"[86] the utility will not be considered an agent of the government for Fourth Amendment purposes. But there might be instances when government instigation will trigger further analysis. If, for example, the government requested the utility to record larger quantities of data than was customary (e.g., increasing the intervals from sub-15 minute intervals to sub-five minute or sub-one minute intervals), this would likely warrant Fourth Amendment scrutiny. Also, if the police requested the utility to hand over customer data, say, for spikes in energy commensurate with a marijuana growing operation, this would likely be a sufficient instigation to trigger further constitutional review. Other situations may arise where the government establishes a dragnet-type law enforcement scheme in which all smart meter data is filtered through police computers. This could also implicate the agency theory and warrant a finding of state action.

Publicly Owned and Operated Utilities

Although the Fourth Amendment (with its warrant and probable cause requirement) typically applies to public actors, in certain instances their collection of information may not fall under the Fourth Amendment or may prompt a lower evidentiary standard. The Supreme Court has infrequently considered the scope of the Fourth Amendment "on the conduct of government officials in noncriminal investigations,"[87] and even less frequently as to "noncriminal *noninvestigatory* governmental conduct."[88] Nonetheless, there are two lines of cases that may apply to smart meters in which the Fourth Amendment may not apply at all (noncriminal noninvestigatory conduct) or may be reduced (noncriminal investigations). The key to this analysis is the government's purpose in collecting the data.

The Supreme Court has developed a line of cases dubbed the "special needs" doctrine that permits the government to perform suspicionless searches if the special needs supporting the program outweigh the intrusion on the individual's privacy.[89] It is premised on the notion that "'special needs,' beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable."[90] If, on the one hand, the objective of the search is not for law

[84] *Id.* at 895.

[85] *Id.* at 904.

[86] United States v. Howard, 752 F.2d 220, 228 (6th Cir. 1985).

[87] *The Supreme Court, 1986-Term—Leading Cases*, 101 HARV. L. REV. 119, 230 (1987).

[88] United States v. Attson, 900 F.2d 1427, 1430 (9th Cir. 1990) (emphasis in original).

[89] Ferguson v. City of Charleston, 532 U.S. 67, 77-78 (2001).

[90] Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 620 (1989) (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987)).

enforcement purposes but for other reasons such as public safety[91] or ensuring the integrity of sensitive government positions,[92] then the doctrine will apply. If, however, the "primary purpose" or "immediate objective" was "to generate evidence *for law enforcement purposes*," then application of the special needs doctrine is not appropriate, and the government must adhere to general Fourth Amendment principles.[93] Again, the primary inquiry is the purpose of the search.

Some circuit courts of appeal have extended the special needs theory, holding that the Fourth Amendment does not apply (in contrast to a reduced standard of suspicion as with the special needs cases) unless the "conduct has as its purpose the intention to elicit a benefit for the government in either its investigative or administrative capacities."[94] In *United States v. Attson*, the Ninth Circuit held that the collection of blood by a government-employed physician, which was subsequently used by the police in a drunk driving prosecution, was not within the scope of Fourth Amendment protection.[95] The panel reasoned that the doctor drew the blood for medical purposes, not to further a governmental purpose in obtaining evidence against the defendant in its criminal investigation, so the Fourth Amendment did not apply.[96]

Applying these two theories to smart meters, a court would focus on the publicly owned utility's purpose in collecting the data. If it were for ordinary business purposes such as billing, informing the customer of its usage patterns, or aiding the utility in making the grid more energy-efficient, then it would not violate the Fourth Amendment. If, however, the public utility began aggregating data at the request of a law enforcement agency, with the purpose of aiding a criminal investigation or other administrative purpose, the Fourth Amendment would seemingly apply. As with private utilities, if the government requested that the public utility report any suspicious electricity usage, or created a program where certain data was regularly transmitted to the police, this might become investigatory and warrant Fourth Amendment protections. It appears law enforcement cannot evade Fourth Amendment restrictions by requesting a publicly owned utility to collect data for it.

Law enforcement might also request smart meter data under a public records theory. It is generally accepted that public records are not accorded Fourth Amendment protection.[97] Unless there is a state or federal statute prohibiting disclosure, "law enforcement access to state public records is unrestricted."[98] Thus the inquiry hinges on whether a document is a public record.

---

[91] *Id.*

[92] Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 670 (1989).

[93] *Ferguson*, 532 U.S. at 83 (emphasis in original).

[94] *See* United States v. Attson, 900 F.2d 1427, 1431 (9th Cir. 1990); Poe v. Leonard, 282 F.3d 123, 137 (2d Cir. 2002); United States v. Elliot, 676 F. Supp. 2d 431, 435-36 (D. Md. 2009).

[95] *Attson*, 900 F.2d at 1433.

[96] *Id.*

[97] *See* Nilson v. Layton City, 45 F.3d 369, 372 (10th Cir. 1995) ("Information readily available to the public is not protected by the constitutional right to privacy."); Doe v. City of New York, 15 F.3d 264, 268 (2d Cir. 1994) ("Certainly, there is no question that an individual cannot expect to have a constitutionally protected privacy interest in matters of public record."); United States v. Ellison, 462 F.3d 557, 562 (6th Cir. 2006) (accessing license plate number from computer database held not an intrusion of a constitutionally protected area, thus not a Fourth Amendment "search"); United States v. Baxter, 492 F.2d 150, 167 (9th Cir. 1973) (holding that Fourth Amendment protections do not extend to telephone company toll and billing records); *see also* Christopher Slobogin, *The Search and Seizure of Computers and Electronic Evidence: Transaction Surveillance by the Government*, 75 MISS. L. J. 139, 156 (2005).

[98] Slobogin, *supra* note 97.

Whether a person's utility records are public records differs from state to state.[99] Some states deem records of a municipally owned and operated electric utility as public records open for public inspection, while others have accorded these records statutory and constitutional protections.

In Florida, for example, records kept in connection with the operation of a city-operated utility are considered public records.[100] A similar policy applies in Georgia, where all records of a government agency, including utility records, must be open for inspection.[101] South Carolina, too, takes a similar approach.[102] It is not clear, however, from the reported cases whether these statutes permit access to personally identifiable information or simply operating records of the utility. Oklahoma is more explicit, permitting access to "records of the address, rate paid for services, charges, consumption rates, adjustments to the bill, reasons for adjustment, the name of the person that authorized the adjustment, and payment for each customer."[103] Oklahoma does protect some confidentiality, including "credit information, credit card numbers, telephone numbers, social security numbers, [and] bank account information for individual customers."[104] Other states, like Washington, specifically protect personally identifiable utility records. Washington does not require a showing of probable cause, but instead "a reasonable belief" that the record will help establish the customer committed a crime.[105] North Carolina likewise states that any "[b]illing information compiled and maintained by a city or county or other public entity providing utility services in connection with the ownership or operation of a public enterprise" is not a public record.[106]

---

[99] Because the focus of this report is federal law and the Fourth Amendment, a full treatment of state privacy law is beyond its scope.

[100] *In re* Public Records—Records of Municipally Operated Utility, Op. Att'y Gen. Fla. 74-35 (1974), *available at* http://www.myfloridalegal.com/ago.nsf/Opinions/B4AED736C2272860852566B30067371A; *see* FLA. STAT. §119.01(1) (2008) ("It is the policy of this state that all state, county, and municipal records are open for personal inspection by any person.").

[101] *See* GA. CODE ANN. §50-18-70(b) (2011); Op. Att'y Gen. Ga. 2000-4 (2000) (requiring personal utility records of certain public employees to be disclosed under public records law). Georgia defines a "public record" as "all documents, papers, letters, maps, books, tapes, photographs, computer based or generated information, or similar material prepared and maintained or received in the course of the operation of a public office or agency." GA. CODE ANN. §50-18-70(a).

[102] In South Carolina, public records include "information in or taken from any account, voucher, or contract dealing with the receipt or expenditure of public or other funds by public bodies." S.C. CODE ANN. §30-4-50 (2011). *See* Kelsey M. Swanson, *The Right to Know: An Approach to Gun Licenses and Public Access to Government Records*, 56 UCLA L. REV. 1579, 1601 (2009).

[103] OKLA. STAT. tit. 51, §24A.10 (2011).

[104] *Id.*

[105] WASH. REV. CODE §42.56.335 (2011). In Washington, the following rule applies to public utility districts and municipally owned electrical utilities:

> A law enforcement authority may not request inspection or copying of records of any person who belongs to a public utility district or a municipally owned electrical utility unless the authority provides the public utility district or municipally owned electrical utility with a written statement in which the authority states that it suspects that the particular person to whom the records pertain has committed a crime and the authority has a reasonable belief that the records could determine or help determine whether the suspicion might be true. Information obtained in violation of this section is inadmissible in any criminal proceeding.

WASH. REV. CODE §42.56.335. The Washington Supreme Court has raised this protection to state constitutional status in *In re* Personal Restraint of Maxfield, 133 Wash. 2d 332, 344 (1997).

[106] However, the North Carolina public records law declares that "[n]othing contained herein is intended to limit public disclosure by a city or county of bill information: ... that is necessary to assist law enforcement, public safety, fire (continued...)

Determining whether a utility is a state actor or whether smart meter data is a public record are merely threshold matters. A finding that an entity is a state actor or data is public does not foreclose law enforcement's ability to retrieve customer smart meter data, but instead activates the next step of Fourth Amendment analysis: whether the government invaded a reasonable expectation of privacy.

Reasonable Expectation of Privacy in Smart Meter Data

Under the modern conception of the Fourth Amendment, the government may not intrude into an area in which a person has an actual expectation of privacy that society would consider reasonable.[107] In the case of smart meter data, the government presumably seeks records in the custody of third-party utilities on the energy use at a specific home. However, a significant body of cases has refused to recognize constitutionally protected privacy interests in information provided by customers to businesses as part of their commercial relationships.[108] This theory, the third-party doctrine, permits police access to the telephone numbers a person dials[109] and to a person's bank documents,[110] free from Fourth Amendment constraints.

There are two relevant differences, however, between smart meters and the traditional third-party cases that may warrant a shift in approach. First is the possible judicial unease with the notion that advancement of technology threatens to erode further the constitutional protection of privacy.[111] From that perspective, as technology progresses, society faces an ever-increasing risk that an individual's activities will be monitored by the government. This is coupled with the concern that the breadth and granularity of personal information that new technology affords provide a far more intimate picture of an individual than the more limited snapshots available through prior technologies. Do the richness and scope of new information technologies warrant increased constitutional scrutiny?

Second, smart meters can convey information about the activities that occur inside the home, an area singled out for specific textual protection in the Fourth Amendment and one deeply ingrained in Anglo-Saxon law.[112] Even when the Court declared that "the Fourth Amendment protects people, not places,"[113] ostensibly shifting away from a property-based conception of the Fourth Amendment, it has still carved out special protections for the home.[114] However, concomitant with the increased use of technology in our private lives is increased exposure of our private activities, including those conducted in the home. Commonly, we share more personal

---

(...continued)

protection, rescue, emergency management, or judicial officers in the performance of their duties." N.C. GEN. STAT. §132-1.1(c)(3).

[107] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[108] *See* Smith v. Maryland, 442 U.S. 735 (1979).

[109] *Id.*

[110] United States v. Miller, 425 U.S. 435 (1976).

[111] Kyllo v. United States, 533 U.S. 27, 33-4 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.").

[112] *See* Entick v. Carrington, 19 How. St. Tr. 1029 (C.P. 1765).

[113] Katz v. United States, 389 U.S. 347, 351 (1967).

[114] *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809-10 (2004) [hereinafter Kerr, *Fourth Amendment and New Technologies*].

information, even as our concerns grow that more individuals, businesses, and others can glean more information about our personal lives as a matter of course. As with technology generally, does the fact that more of our lives are becoming "public" call for lesser or greater constitutional protection, and how does a "reasonable expectation"-based model continue to apply in a technologically intensive society?

This subpart will first look at the third-party doctrine as it is commonly conceived by the courts. Then it will discuss whether there are sufficient differences between the use of smart meters and traditional third-party cases to counsel against its application.

Third-Party Doctrine

Traditionally, there has been no Fourth Amendment protection for information a consumer gives to business as part of their business dealings.[115] This doctrine dates back to the secret agent cases, in which any words uttered to another person, including a government agent or informant, were not covered by the Fourth Amendment.[116] It was later extended to business records, giving police access to documents such as telephone records,[117] bank records,[118] motel registration records,[119] and cell phone records.[120] The Supreme Court has reasoned that the customers assume the risk that the information could be handed over to government authorities,[121] and also that they consent to such access.[122] Some lower courts have applied this theory to traditional analog utility meters.[123] This section discusses the possible application of the third-party doctrine to smart meters.

In *Miller v. United States*, agents of the Bureau of Alcohol, Tobacco, and Firearms (ATF) subpoenaed several banks for records pertaining to the defendant, including copies of the defendant's checks, deposit slips, and financial statements.[124] The defendant moved to suppress the records at trial, arguing that a warrantless retrieval of the bank records (his "private papers")[125] was an intrusion into an area protected by the Fourth Amendment. The Court

---

[115] Orin S. Kerr, *The Case for a Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009) [hereinafter Kerr, *Third-Party Doctrine*]. While the third-party doctrine has supporters like Professor Kerr, this group is overshadowed by its vocal detractors. Professor LaFave described its underpinnings as "dead wrong" and that the "Court's woefully inadequate reasoning does great violence to the theory of Fourth Amendment protection which the Court developed in *Katz*." LAFAVE, *supra* note 78, §2.7(c). Justice Sotomayor lent credence to this sentiment in *United States v. Jones*, where she posited that it "may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." United States v. Jones, 565 U.S. ___, 5 (Sotomayor, J., concurring in the judgment and the opinion).

[116] United States v. White, 401 U.S. 745, 750 (1971) (holding that the Fourth Amendment "affords no protection to a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.") (internal quotation marks omitted).

[117] Smith v. Maryland, 442 U.S. 735 (1979).

[118] United States v. Miller, 425 U.S. 435 (1976).

[119] United States v. Willis, 759 F.2d 1486, 1498 (11th Cir. 1985).

[120] United States v. Hynson, No. 05-576, 2007 WL 2692327, at *6 (E.D. Pa. Sept. 11, 2007).

[121] *Smith*, 442 U.S. at 744.

[122] Kerr, *Third-Party Doctrine*, *supra* note 115.

[123] United States v. McIntyre, 646 F.3d 1107 (8th Cir. 2011).

[124] *Miller*, 425 U.S. at 437-438.

[125] Brief for Respondent at 4, *Miller*, 425 U.S. 435 (No. 74-1179), 1975 WL 173642, at *4 ("The Fourth Amendment is historically rooted in a concern for control over personal and private information in the face of governmental demands (continued...)

disagreed, broadly declaring "the Fourth Amendment does not prohibit the obtaining of information revealed to a third-party and conveyed by him to Government authorities, even if it is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third-party will not be betrayed."[126] The Court further noted that "the depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[127]

Three years later, the Court extended the third-party doctrine to outgoing numbers dialed from a person's telephone.[128] In *Smith v. Maryland*, the defendant robbed a woman and began making obscene phone calls to her.[129] Suspecting Smith placed the calls, the police used a pen register to track the telephone numbers dialed from his phone.[130] The police failed to obtain a warrant or subpoena before installing the pen register.[131] The register revealed that Smith was in fact making the phone calls to the woman. In denying Smith's motion to suppress, the Court relied on the third-party doctrine, stating that "this Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[132] As applied to the telephone context, the Court found that "[w]hen he used his phone, [Smith] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, [Smith] assumed the risk that the company would reveal to police the numbers he dialed."[133]

Traditionally, utility records have been handled similarly to bank records and telephone records. Several lower federal courts have held that customers do not have a reasonable expectation of privacy in their utility records, thereby permitting warrantless access to these records. In *United States v. Starkweather*, the Ninth Circuit held that a person does not have a reasonable expectation of privacy in his utility records.[134] The panel reasoned that (1) these records were no different from phone records, and thus did not justify a different constitutional result; and (2) the public was aware that such records were regularly maintained, thereby negating any expectation of privacy.[135] The Eighth Circuit has also upheld warrantless police access to utility records in *United States v. McIntyre*.[136] The Eighth Circuit panel distinguished *Kyllo*, declaring that the means of obtaining the information in *Kyllo* (a thermal-imaging device) was significantly more intrusive than simply subpoenaing the records from the utility company.[137] The court held that "the means to obtaining the information is legally significant."[138] Likewise, the court in *United*

(...continued)

for access and use.") (citing Entick v. Carrington, 19 How. St. Tr. 1029 (C.P. 1765)).

[126] *Miller*, 425 U.S. at 443.

[127] *Id.*

[128] Smith v. Maryland, 442 U.S. 735 (1979).

[129] *Id.* at 737.

[130] *Id.*

[131] *Id.*

[132] *Id.* at 743-44.

[133] *Id.* at 744.

[134] United States v. Starkweather, No. 91-30354, 1992 WL 204005, at *2 (9th Cir. Aug. 24, 1992).

[135] *Id.*

[136] United States v. McIntyre, 646 F.3d 1107 (8th Cir. 2011).

[137] *Id.* at 1111.

[138] *Id.*

States v. Hamilton held that the means of obtaining power records from a third-party by way of administrative subpoena as opposed to "intrusion on the home by 'sense enhancing technology'" is "legally significant," removing this type of situation from the *Kyllo*-home privacy line of cases into the *Miller*-third-party line.[139]

It is difficult to predict whether a court would extend this traditional third-party analysis to smart meters. The courts may seek to ensure the predictability and stability of the third-party doctrine generally and administration of utility services specifically, thus requiring a bright-line rule for all third-party circumstances.[140] There is an advantage to a rule that is easy to apply, that allows utilities to better govern their affairs, and does not permit "savvy wrongdoers [to] use third-party services in a tactical way to enshroud the entirety of their crimes in zones of Fourth Amendment protection."[141] However, there are three overarching considerations embodied in the use of smart meters that might weigh against the application of traditional third-party analysis. These include (a) a person's expectation of privacy while at home; (b) the breadth and granularity of private information conveyed by smart meters; (c) the lack of a voluntary assumption of the risk or consent to release of this data.

Privacy in the Home

The location of the search mattered little in the traditional third-party cases, but it may take on constitutional significance with smart meters.[142] In the case of smart meters, the information is generated in the home, an area accorded specific textual protection in the Fourth Amendment, and one the Supreme Court has persistently safeguarded.[143] In no uncertain terms the Court has asserted that "[a]t the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable government intrusion."[144] Even as technology advances—whether a tracking or thermal-imaging device or something new—the Court has maintained this bulwark. Because of the significance of the home, access to smart

[139] United States v. Hamilton, 434 F. Supp. 2d 974, 980 (D. Or. 2006); Booker v. Dominion Va. Power, No. 3:09-759, 2010 U.S. Dist. LEXIS 44960, at *17 (E.D. Va. May 7, 2010); *see also* Samson v. State, 919 P.2d 171, 173 (Ala. App. 1996) (holding under state constitution that "utility records are maintained by the utility and do not constitute information in which society is prepared to recognize a reasonable expectation of privacy"); People v. Stanley, 86 Cal. Rptr. 2d 89, 94 (Cal. App. 1999) (same).

[140] *See* Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1687, 1710 (1976).

[141] Kerr, *Third-Party Doctrine*, *supra* note 115, at 564.

[142] In *Smith*, the "site of the call was immaterial for purposes of analysis" of that case. Smith v. Maryland, 442 U.S. 735, 743 (1979). Whether a person dials a telephone number from his home, a telephone booth, or any other location does not alter the nature of the activity, and thus does not affect the Fourth Amendment analysis. The privacy interests implicated are the same no matter where the call is placed. The same theory applies to bank records. It matters not where someone writes a check, or fills out a deposit slip—the privacy interest is the same.

[143] Payton v. New York, 445 U.S. 573, 589 ("The Fourth Amendment protects the individual's privacy in a variety of settings. In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home—a zone that finds its roots in clear and specific constitutional terms: 'The right of the people to be secure in their ... houses ... shall not be violated.'") (quoting U.S. CONST. amend IV); Minnesota v. Carter, 525 U.S. 83, 99 (1998) (Kennedy, J., concurring) ("[I]t is beyond dispute that the home is entitled to special protection as the center of the private lives of our people. Security of the home must be guarded by law in a world where privacy is diminished by enhanced surveillance and sophisticated communication systems.").

[144] Silverman v. United States, 365 U.S. 505, 511 (1961).

meter data may prompt a doctrinal shift away from the third-party doctrine. Several home privacy cases shed light on this possible approach.[145]

In *Kyllo v. United States*, the Court had to decide whether the use of a thermal-imaging device from the outside of a home that detected the amount of heat coming from inside the home was a violation of the Fourth Amendment.[146] In *Kyllo*, an agent of the Department of the Interior suspected Danny Kyllo was growing marijuana in his home with the use of high-intensity lamps.[147] The agent used a thermal imager to scan the outside of Kyllo's apartment to determine if he was using these "grow" lamps.[148] Thermal imagers can detect energy emitting from the outside surface of an object.[149] When scanning the home, the thermal imager produced an image with various shades of black, white, or gray—the shades darker or lighter depending on the warmth of the area being scanned.[150] From the passenger seat of his car, the agent scanned Kyllo's home for several minutes.[151] From his scan, he determined that the area over the garage and one side of his home were relatively hot compared to neighboring homes.[152] Based on utility bills, informant tips, and the results of thermal imaging, the agents obtained a warrant to search Kyllo's home.[153] As suspected, inside the home the agents found a marijuana growing operation, including over 100 plants.[154]

Justice Scalia first posited that "with very few exceptions, the question whether a warrantless search of the home is reasonable must be answered no."[155] Searches of the home were historically analyzed under the common law doctrine of trespass,[156] but during the mid-20th century the Court instead anchored the Fourth Amendment to a conception of privacy.[157] While this test may be difficult to apply in the context of automobiles, telephone booths, or other public areas, it is made easier when concerning the home:

> In the case of the search of the interior of homes—the prototypical and hence most commonly litigated area of protected privacy—there is a ready criterion, with deep roots in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged

---

[145] In April 2012, the Supreme Court will hear oral arguments in its most recent home privacy case, Jardines v. Florida, 73 So. 3d 34 (Fla. 2011), *cert granted*, 2012 U.S. LEXIS 7 (Jan. 6, 2012) (No. 11-564), where it will decide whether a drug sniff at the front door of a suspect's house by a trained narcotics dog is a Fourth Amendment search requiring probable cause. This case should shed further light on the parameters of privacy surrounding the home.

[146] Kyllo v. United States, 533 U.S. 27, 29 (2001).

[147] *Id.*

[148] *Id.*

[149] *Id.*

[150] *Id.* at 29-30.

[151] *Id.* at 30.

[152] *Id.*

[153] *Id.*

[154] *Id.* The Ninth Circuit held that Kyllo had not exhibited a subjective expectation of privacy in the home because he did not attempt to prevent the heat emitting from the lamps from escaping his home. United States v. Kyllo, 190 F.3d 1041, 1046 (9th Cir. 1999). Further, the panel held that even if he had a subjective expectation of privacy, it was not a reasonable one since the imager "did not expose any intimate details of Kyllo's life." *Id.* at 1047.

[155] *Kyllo*, 533 U.S. at 31.

[156] *See* Olmstead v. United States, 277 U.S. 438 (1928).

[157] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The modern formulation of the reasonable expectation of privacy test derives not from the majority opinion but from Justice Harlan's concurrence.

> to be reasonable. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment.[158]

The Court ultimately held that "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search—at least where (as here) the technology in question is not in general public use."[159] *Kyllo* affirmed the notion that "an expectation of privacy in activities taking place inside the home is presumptively reasonable."[160]

The Court also protected home privacy by prohibiting the monitoring of the location of a beeper while inside a residence.[161] In *United States v. Karo*, with the consent of a government informant the police attached a beeper to the false bottom of a can of ether, which was sold to Karo.[162] The can of ether was transported between several residences and storage facilities.[163] The police used the beeper to monitor the location of the can several times while it was located inside of the residences.[164] The Court was asked to determine "whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence."[165] The Court answered in the affirmative.

The Court reiterated the long-standing notion that "private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable."[166] Unless there are exigent circumstances, "searches and seizures inside a home without a warrant are presumptively unreasonable...."[167] The Court ultimately held that the warrantless monitoring of the beeper in the home was a Fourth Amendment violation.[168]

Kyllo and *Karo* demonstrate that the Supreme Court "has defended the home as a sacred site at the 'core of the Fourth Amendment.'"[169] Although neither the Supreme Court nor any lower federal court has ruled on the use of smart meters, a few propositions can be deduced from *Kyllo* and *Karo* bearing on this question.

Because smart meters allow law enforcement to access information regarding intimate details occurring inside the home, a highly invasive investigation that could not otherwise be performed without intrusion into the home, a court may require a warrant to access this data. In *Kyllo*, the

---

[158] *Kyllo*, 533 U.S. at 34.

[159] *Id.* (internal quotation marks omitted).

[160] Lerner & Mulligan, *supra* note 60, ¶ 18.

[161] United States v. Karo, 468 U.S. 705 (1984).

[162] *Id.* at 708.

[163] *Id.*

[164] *Id.* at 709-10.

[165] *Id.*

[166] *Id.* at 714.

[167] *Id.* at 714-15.

[168] *Id.* at 718.

[169] Stephanie M. Stern, *The Inviolate Home: Housing Exceptionalism in the Fourth Amendment*, 95 CORNELL L. REV. 905, 913 (2010) (citing Wilson v. Layne, 526 U.S. 603, 612 (1999)).

police merely obtained the relative temperatures of a house,[170] and in *Karo* the police only generally located the beeper in the house.[171] Although this information was limited, the Court nonetheless prohibited such investigatory techniques. Smart meters have the potential to produce significantly more information than that derived in *Kyllo* and *Karo*, including what individual appliances we are using; whether our house is empty or occupied; and when we take our daily shower or bath.[172] Further, a look at **Figure 1**, *supra*, makes it clear that this level of information is much more intimate than prior technologies used by law enforcement. This depth of intrusion suggests that customers may have a reasonable expectation of privacy in smart meter data.

There is also a question whether smart meters are in "general public use." (The police must use technology not in general public use for *Kyllo* to apply.)[173] Unfortunately, the Court provided no criterion for making this determination.[174] Several courts applying this test have held that night vision goggles were in general public use.[175] One federal district court reasoned that the goggles were regularly used by the military and police and could be found on the Internet, so were considered in general public use.[176] In 2009, the Department of Energy estimated that 4.75% of all electric meters were smart meters.[177] The department projects that by 2012 approximately 52 million more meters will be installed.[178] With little guidance on this issue, it is uncertain whether this jump in numbers would elevate smart meters into the general public use category.

The means by which data is gathered also differentiates the thermal-imaging in *Kyllo* from smart meters. In *Kyllo*, the police independently gathered the information using the thermal imager; an agent went outside Kyllo's house and used the thermal imager himself.[179] With smart meters, the utility company compiles the information and the police subpoena the company for the data. This difference in means was material in one lower court analyzing access to traditional utility data.[180] It is not clear whether this difference advises against application of *Kyllo* here.

Mosaic and Dragnet Theories

The second factor guiding against the application of the third-party doctrine is composed of two interconnected theories: the mosaic and dragnet theories. The mosaic theory is grounded in the idea that surveillance of the whole of one's activities over a prolonged period is substantially

[170] United States v. Kyllo, 533 U.S. 27, 30 (2001).

[171] *Karo*, 468 U.S. at 705, 709-10.

[172] NIST PRIVACY REPORT, *supra* note 11, at 14 & n.35. It is unclear whether the specificity of the data from the smart meter will directly affect the constitutional analysis. *Kyllo*, 533 U.S. at 37 ("The *Fourth Amendment's* protection of the home has never been tied to measurement of the quality or quantity of information obtained."). With that said, the NIST report maintains that sufficient information about the activities inside of the home are presented to implicate a *Kyllo*, home search analysis.

[173] *Kyllo*, 533 U.S. at 34.

[174] *See* Douglas Adkins, *The Supreme Court Announces a Fourth Amendment "General Public Use" Standard for Emerging Technologies but Fails to Define It:* Kyllo v. United States, 27 DAYTON L. REV. 245 (2002).

[175] *See* United States v. Dellas, 355 F. Supp. 2d 1095, 1107 (N.D. Cal. 2005).

[176] United States v. Vela, 486 F. Supp. 2d 587, 590 (W.D. Tex. 2005).

[177] DEP'T OF ENERGY, SMART GRID SYSTEM REPORT vi (2009), *available at* http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/SGSRMain_090707_lowres.pdf.

[178] *Id.*

[179] United States v. Kyllo, 533 U.S. 27, 29 (2001).

[180] United States v. McIntyre, 646 F.3d 1107, 1111-12 (8th Cir. 2011).

more invasive than a look at each item in isolation.[181] In the case of smart meters, this is the difference between knowing a person's monthly energy usage, and being able to discern a person's daily activities with considerable accuracy. This theory intersects with dragnet-styled law enforcement techniques in which the police cast a wide surveillance net, taking in a wealth of personal information with the goal of finding criminal activity among the stream of data.

Although the Supreme Court has never formally adopted the mosaic theory, there seems to be a ready-made majority potentially willing to consider it.[182] In *United States v. Jones*, the police used a GPS tracking device to track Jones's movements for almost a month.[183] The majority, led by Justice Scalia, held that attaching a GPS device on a vehicle for the purpose of collecting information constituted a "search" under the Fourth Amendment.[184] The physical intrusion, rather than a *Katz*-type invasion of privacy, was the lynchpin of the decision.[185] Justices Alito and Sotomayor both agreed that this was a search, but on different grounds. Both discussed an adaptation of the mosaic theory as prohibiting police from tracking a person for an extended period of time. Justice Alito, joined by Justices Breyer, Ginsburg, and Kagan, assumed that a short-term search would not violate the Fourth Amendment, but that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[186] Likewise, Justice Sotomayor agreed with this "incisive" observation, noting that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about familial, political, professional, religious, and sexual associations."[187] Both of these comments closely mirror those of the opinion below, which relied on the mosaic theory: "A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts."[188]

Although the *Jones* majority did not embrace the mosaic theory, the concurrences demonstrate that five justices are flirting with the idea. These arguments resemble those made against the unfettered use of smart meter data. With smart meters, police would have a rich source of personal data that reveals far more about a person than traditional analog meters. Understanding a person's daily activities, including what appliances he is using, is a far leap from knowing his monthly energy usage. This is the difference between knowing about a single trip a person took and monitoring his movements over a month-long period. The breadth and granularity of the smart meter data may be seen as warranting application of the mosaic theory and may perhaps find receptive ears on the Court.

Additionally, the dragnet theory may apply to collection of energy usage data. This theory states that surveillance normally permitted under the Fourth Amendment—such as monitoring a person's movements on a public street—becomes an impermissible invasion of privacy when

---

[181] *See* Cent. Intelligence Agency v. Sims, 471 U.S. 159, 178 (1985).

[182] *See* Orin Kerr, VOLOKH CONSPIRACY, What's the Status of the Mosaic Theory After Jones?, http://volokh.com/2012/01/23/whats-the-status-of-the-mosaic-theory-after-jones/.

[183] United States v. Jones, 565 U.S. ___, 2 (2012).

[184] *Id.* at 3.

[185] *Id.* at 4.

[186] *Id.* at 13 (Alito, J., concurring in the judgment).

[187] *Id.* at 3 (Sotomayor, J., concurring in the judgment and the opinion).

[188] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

conducted on a prolonged, 24-hour basis.[189] "If such dragnet-type law enforcement practices as respondent envisions should eventually occur," Justice Rehnquist asserted earlier in *United States v. Knotts*, "there will be time enough then to determine whether different constitutional principles may be applicable."[190] Twenty-four hour access to our intimate daily activities, including what appliances we use, when we take our daily shower or bath, eat, and sleep, may push smart meters into the dragnet category.

Coinciding with the mosaic and dragnet theories is the difference in sophistication and the quantity of the data revealed between traditional third-party cases and smart meters. Comparing *Smith* with *Katz* provides insight into this distinction. Pen registers, as used in *Smith*, have "limited capabilities"—they can only record the numbers dialed from a phone.[191] In comparison, in *Katz* the police listened to the contents of Katz's phone call—the actual words spoken.[192] In noting this distinction, it seems the *Smith* Court, in permitting the use of pen registers, intentionally limited its holding to the discrete set of data conveyed—the telephone numbers dialed. Smart meters, to the contrary, have the potential to collect and aggregate precise detail about the activities inside the home. It is more than one packet of data, but reveals minute-by-minute activity, something far more revealing, and arguably more like *Katz* than *Smith*.

Assumption of the Risk—Consent

The third difference between traditional third-party cases and smart meters is the nature of services involved and whether the customer actually assumes the risk or consents to this information being shared with others. Assumption of the risk and consent are the two leading theories supporting the third-party doctrine. In *United States v. Miller*, the customer "assumed the risk" that the bank would turn over the bank records to government authorities.[193] That was a risk he took in doing business with the bank. As to the consent theory, one commentator asked and answered the question as follows: "When does a person's choice to disclose information to a third-party constitute consent to a search? So long as a person knows that they are disclosing information to a third-party, their choice to do so is voluntary and the consent valid."[194]

With banking or telephone services, a customer has the option of transferring his business to another bank or another telephone carrier.[195] To the contrary, because electric utilities are essentially monopolies, the customer cannot simply switch services. The only way to avoid the recordation of his electric usage is to terminate his utility service altogether, an impracticable option in modern society. As one state court has noted:

> Electricity, even more than telephone service, is a "necessary component" of modern life, pervading every aspect of an individual's business and personal life: it heats our homes,

[189] *Id.* at 558.

[190] United States v. Knotts, 460 U.S. 276, 283-84 (1983). Because this statement was not essential to the holding, it was dictum: persuasive, but not binding.

[191] *Smith*, 442 U.S at 741 (citing Katz v. United States, 389 U.S. 347 (1967)).

[192] *Katz*, 389 U.S. at 348.

[193] *Smith*, 442 U.S. at 744 (citing United States v. Miller, 425 U.S. 435 (1976)).

[194] Kerr, *Third-Party Doctrine*, *supra* note 115, at 588.

[195] *Contra Smith*, 442 U.S. at 750 (Marshall, J., dissenting) ("[U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of "assuming" the risk in contexts where, as a practical matter, individuals have no realistic alternative.").

> powers our appliances, and lights our nights. A requirement of receiving this service is the disclosure to the power company (and in this case an agent of the state) of one's identity and the amount of electricity being used. The nature of electrical service requires the disclosure of this information, but that disclosure is only for the limited business purpose of obtaining the service.[196]

It is not clear whether assumption of the risk or consent should apply to smart meters. It is reasonable to assume that customers understand utility companies must collect usage data to bill the customer for that usage. Customers receive their statement each month demonstrating this fact. However, most customers are probably not familiar with the sophistication of smart meters and the detailed data sets that can be derived from them. Even if customers are aware their utility usage can be recorded in sub-fifteen minute intervals, a reasonable customer would probably be surprised, if not shocked, to know that data from smart meters can potentially be used to pinpoint the usage of specific appliances. If knowledge of the sophistication of the data is a prerequisite to assumption of the risk or consent, it is difficult to say whether a reasonable customer would understand the privacy implications with this new technology.[197]

Because smart meters are an emerging technology not yet judicially tested, it is difficult to conclude with certainty how they would be handled under the Fourth Amendment. Further, beyond the possible constitutional implications of smart meters, federal communication and privacy statutes may also apply. As noted by Professor Kerr, "in recent decades, legislative privacy rules governing new technologies have proven roughly as privacy protective, and quite often more protective than, parallel Fourth Amendment rules."[198]

Statutory Protection of Smart Meter Data

This section discusses federal statutory protections that may be applicable to the contents of communications sent by a smart meter, independent of the Fourth Amendment, while they are either stored within the smart meter prior to transmission, during transmission, or after they have been delivered to the utility. Three federal laws, the Electronic Communications Privacy Act (ECPA),[199] the Stored Communications Act (SCA),[200] and the Computer Fraud and Abuse Act (CFAA)[201] may be applicable to these situations and are discussed in more detail below.

---

[196] *In re* Restraint of Maxfield, 133 Wn.2d 332, 341 (Wash. 1997); *see also* Balough, *supra* note 63, at 185.

[197] *Cf.* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("*Miller* involved simple business records, as opposed to the potentially unlimited variety of 'confidential communications' at issue here.").

[198] Kerr, *Fourth Amendment and New Technologies*, *supra* note 114, at 806.

[199] For more detailed information on ECPA, *see* CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle.

[200] For a more detailed discussion of the SCA, *see* CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle.

[201] For more detailed information on the CFAA, *see* CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle.

The Electronic Communications Privacy Act (ECPA)

ECPA, enacted in 1986, "addresses the interception of wire, oral and electronic communications."[202] The statute defines electronic communications as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce...."[203] Based on the description of the smart meter network provided above,[204] the envisioned transmission of customers' energy usage data by smart meters would seem to fall squarely within the definition of electronic communications under ECPA.

ECPA generally prohibits the interception of electronic communications, but also provides a mechanism for government entities to conduct such surveillance, and a number of other exceptions.[205] Additionally, the statute provides that interception under the procedures and exceptions set forth in ECPA, or pursuant to the Foreign Intelligence Surveillance Act, are the exclusive means for intercepting electronic communications.[206] The unlawful interception of electronic communications in violation of ECPA is generally punishable by imprisonment for not more than five years and/or a fine of not more than $250,000 for individuals and not more than $500,000 for organizations.[207]

Of particular relevance to the immediate discussion is the fact that ECPA permits interception of an electronic communication where a party to the communication has consented to such interception.[208] In the context of a smart meter network that is the subject of this report, it appears that the utility would be a party to all of the communication sent by the smart meters, since it is primarily receiving that information for its own billing purposes. Therefore, if the utility consents to law enforcement's interception of the traffic which is addressed to it, that surveillance would not appear to violate the prohibitions in ECPA.

ECPA also provides a procedural mechanism for law enforcement to conduct surveillance activities for investigative purposes without the consent of any party to the communication. The statute limits the types of criminal cases in which electronic surveillance may be used[209] and requires court orders authorizing electronic surveillance to be supported by probable cause to believe that the target is engaged in criminal activities, that normal investigative techniques are

---

[202] S.Rept. 99-541 at 3.

[203] 18 U.S.C. §2510(12).

[204] *See supra* note 47 and accompanying text (noting that smart meters may use a variety of communications technologies, including fiber optics, wireless networks, satellite, and broadband over power line).

[205] 18 U.S.C. §2516. Exceptions cover things such as interception with the consent of a party to the communication and interception by communication service providers as an incident to providing service.

[206] 18 U.S.C. §2511(2)(f). FISA defines electronic surveillance to include more than the interception of wire, oral, or electronic communications, 50 U.S.C. §1801(f), but places limitations on its definition based upon the location or identity of some or all of the parties to the communications involved.

[207] "Except as provided in (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both." 18 U.S.C. §2511(4)(a).

[208] 18 U.S.C. §2511(2)(c).

[209] The list of covered criminal provisions can be found at 18 U.S.C. §2516(1), and includes offenses such as violence at international airports; animal enterprise terrorism; arson; bribery of public officials and witnesses; unlawful use of explosives; fraud by wire, radio, or television; terrorist attacks against mass transportation; sexual exploitation of children; narcotics production and trafficking; and many others.

insufficient, and that the facilities that are the subject of surveillance will be used by the target.[210] It also limits the use and dissemination of information intercepted.[211] In addition, when an interception order expires, authorities must notify those whose communications have been intercepted.[212] Law enforcement may also conduct electronic surveillance when acting in an emergency situation pending issuance of a court order.[213]

The government may also conduct electronic surveillance under the authority of the Foreign Intelligence Surveillance Act (FISA). FISA governs the gathering of information about foreign powers, including international terrorist organizations, and agents of foreign powers.[214] Although it is often discussed in relation to the prevention of terrorism, it applies to the gathering of foreign intelligence information for other purposes.[215] Although some exceptions apply, such as for emergency situations,[216] the government typically must obtain a court order, supported by probable cause, from the Foreign Intelligence Surveillance Court (FISC), a neutral judicial decision maker, in order to conduct electronic surveillance pursuant to FISA.[217]

The Stored Communications Act (SCA)

The SCA was enacted in 1986 as Title II of the Electronic Communications Privacy Act (ECPA),[218] to "address[] access to stored wire and electronic communications and transactional records."[219] The SCA prohibits unauthorized persons from accessing a facility through which an *electronic communication service* (ECS) is provided; or obtaining, altering, or preventing access to an electronic communication while it is in *electronic storage* in an ECS.[220] The SCA also limits the circumstances in which providers of ECS or a *remote computing service* (RCS) may disclose information that they carry or maintain.[221] The SCA also provides a mechanism by which law enforcement may compel the disclosure of stored communications.[222]

The terms "electronic communication service," "remote computing services," and "electronic storage" are all specifically defined by the SCA. As described above, the SCA applies only to providers of either an ECS or an RCS; stored communications held by other types of entities are not protected by the SCA. Therefore, in order to determine whether the SCA would protect stored information collected by a smart meter, this report will first examine whether a utility's deployment of a smart meter network falls within the definition of an ECS or an RCS and then

[210] 18 U.S.C. §§2516, 2518(3).

[211] 18 U.S.C. §2517.

[212] 18 U.S.C. §2518(8).

[213] 18 U.S.C. §2518(7).

[214] *See* 50 U.S.C. §1801(a) (definition of "foreign power").

[215] For example, it extends to the collection of information necessary for the conduct of foreign affairs. *See* 50 U.S.C. §1801(e) (definition of "foreign intelligence information").

[216] 50 U.S.C. §1805(e).

[217] 50 U.S.C. §§1801-1808. FISA authorizes electronic surveillance without a FISA order in specified instances involving communications between foreign powers. 50 U.S.C. §1802.

[218] P.L. 99-508.

[219] S.Rept. 99-541 at 3.

[220] 18 U.S.C. §2701(a). Unauthorized access includes exceeding an authorization to use the facility. *Id.*

[221] 18 U.S.C. §2702.

[222] 18 U.S.C. §2703.

discuss the protections and disclosure restrictions that might apply to any smart meter network that qualifies as an ECS or RCS.

Electronic Communication Services

An ECS is defined by the SCA as any service which provides users "the ability to send or receive wire or electronic communications."[223] The statute also defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[224] As described above, one of the essential functions of a smart meter would appear to be the capability to transmit consumer electricity usage data to the smart grid using a variety of communications technologies.[225] These transmissions would seem to fall neatly within the SCA's definition of an electronic communication. Therefore, whether a smart meter network would qualify as an ECS would likely depend on whether the deployed smart meters could be said to be providing this ability to users.

It is not clear whether it would be accurate to categorically describe smart meters as providing customers with "the ability to send or receive" communications. It could be argued that a utility customer would use the smart meter to transmit usage information to the utility, in the same way that the same customer uses a traditional meter to record household electricity usage over a billing period. However, the Ninth Circuit has suggested that an ECS should not include situations in which electronic communications are used only "as an incident to providing some other service, as is the case with a street-front shop that requires potential customers to speak into an intercom device before permitting entry, or a 'drive-thru' restaurant that allows customers to place orders via a two-way intercom located beside the drive-up lane."[226] On one hand, it may not be accurate to describe utility customers as users of smart meters at all, particularly if the deployment of such smart meters is intended principally for the benefit of the utility and does not change the experience of utility customers. On the other hand, some of the proposed uses of deployed smart meters may include using collected data for the benefit of the customers, for example by determining the energy efficiency of specific household appliances.[227] As a result, the ultimate classification of a particular smart meter network as an ECS may depend largely on the specific facts present, such as the manner in which it is marketed, or the ostensible purposes for which the transmissions are intended to be used.

If a smart meter network qualifies as an ECS, then transmissions containing smart meter data would be protected under the SCA only while such transmissions are in electronic storage, as that term is defined by the statute.[228] Therefore, one must first determine whether, and under what circumstances, the data collected by a smart meter network is in electronic storage in order to determine what protections apply.

---

[223] 18 U.S.C. §2510(15).

[224] 18 U.S.C. §2510(12). Wire communications are defined as communications containing the human voice and are not implicated here. 18 U.S.C. §2510(1).

[225] *See supra* note 47 and accompanying text.

[226] Company v. United States (*In re* United States), 349 F.3d 1132, 1141 (9th Cir. 2003) (holding that definition of ECS includes service that provides drivers with the ability to make phone calls from their car for directory assistance, driving directions, or roadside assistance because those activities are intrinsically communicative).

[227] *See supra* note 8.

[228] 18 U.S.C. §2701.

For purposes of the SCA, a communication is in electronic storage at an ECS if it is in temporary, intermediate storage incidental to electronic transmission or in storage for backup protection.[229] As applied to the smart meter network, data residing on the smart meter itself prior to being sent to the utility would appear to be in electronic storage, as such storage is likely temporary and undertaken solely in anticipation of some eventual transmission to the utility. In contrast, once the data has arrived at the utility and resides on its servers, it may no longer be in temporary or intermediate storage. However, some form of the communications may still be being held for backup purposes, and in such a case might be considered in electronic storage under the statute. To the extent that the data would be considered in electronic storage, either while on the meter or on the utility's computers, the data would appear to be subject to the SCA's provisions applicable to providers of ECS.

The SCA prohibits intentionally accessing without authorization, a facility through which an ECS is provided and obtaining, altering, or preventing access to an electronic communication while it is in electronic storage.[230] Criminal penalties for violating the SCA's prohibitions on unauthorized access start at imprisonment for not more than one year (not more than five years for a subsequent conviction) and/or a fine of not more than $100,000.[231] However, violations committed for malicious, mercenary, tortious or criminal purposes are subject to higher penalties and may be punished by imprisonment for not more than five years (not more than 10 years for a subsequent conviction) and/or a fine of not more than $250,000 (not more than $500,000 for organizations).[232] Victims of a violation of the SCA also have a civil cause of action for equitable relief, reasonable attorneys' fees and costs, and damages equal to the loss and gain associated with the offense but not less than $1,000.[233]

The SCA generally restricts the ability of providers of ECS to disclose the contents of communications in electronic storage, if the ECS is offering those services to the public.[234] However, the statute also permits certain disclosures to law enforcement. Such permitted disclosures by a provider of electronic communication services to law enforcement can be either voluntary or compelled. Normally, voluntary disclosure to law enforcement is authorized only if the contents of the communication were inadvertently obtained by the service provider and appear to pertain to the commission of a crime.[235] However, it should be noted that the utility in this case appears to be the intended recipient of all communications sent over the smart meter network, and the SCA's restrictions on disclosures of electronically stored information held by ECS or RCS providers may generally be overcome if an intended recipient of the communication consents to the disclosure.[236] Consequently, the utility may have more latitude to share communications in electronic storage with law enforcement than a traditional provider of ECS, such as a telephone company, would have.

---

[229] 18 U.S.C. §2510(17).

[230] 18 U.S.C. §2701(a). Unauthorized access includes exceeding an authorization to use the facility. *Id.*

[231] 18 U.S.C. §2701(b)(2).

[232] 18 U.S.C. §2701(b)(1).

[233] 18 U.S.C. §2707.

[234] 18 U.S.C. §2702(a)(1) ("a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service").

[235] 18 U.S.C. §2702(b)(7).

[236] *See* 18 U.S.C. §2702(b)(3).

For purposes of compelled disclosures to law enforcement, the SCA distinguishes between recent communications and those that have been in electronic storage for more than 180 days. A search warrant is required to compel providers to disclose communications held in electronic storage for 180 days or less.[237] However, communications held for more than 180 days may be obtained by law enforcement through a warrant, subpoena, or a court order supported by specific and articulable facts sufficient to establish reasonable grounds to believe that the contents are relevant and material to an ongoing criminal investigation.[238] Customers whose communications have been disclosed are generally required to be given notice of such disclosure, but such disclosure may be delayed if notification might result in endangering the life or physical safety of an individual; flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; or otherwise seriously jeopardizing an investigation or unduly delaying a trial.[239]

Remote Computing Services

It is likely that the classification of a smart meter network as an RCS would similarly be fact-dependent. The SCA defines an RCS as a service in which computer storage or processing services by means of an ECS are provided to the public.[240] It is conceivable that the data collected by smart meters may in fact be stored or processed by the utility, but there is no indication that such storage or processing would be categorically provided as a service to the public, rather than solely for the utility's internal benefit.[241] If such service is not provided to the public, then it would likely be inaccurate to classify the smart meter network as an RCS. However, if one of the features of a particular smart meter deployment is to give customers the ability to store or process their usage data, then it would appear to qualify as an RCS.

For those smart meter networks which qualify as an RCS, the SCA generally protects the contents of electronically transmitted communications "carried or maintained on that service" for customers of the service. Disclosures of such information are generally prohibited,[242] but the SCA also provides a means for law enforcement to obtain access to the contents of such communications. The government may obtain a warrant supported by probable cause, or use a subpoena or a court order supported by specific and articulable facts sufficient to establish reasonable grounds to believe that the contents are relevant and material to an ongoing criminal investigation.[243] However, use of a subpoena or court order supported by specific and articulable facts also requires the government to give prior notice to the customer whose information is sought, unless particular circumstances warrant delayed notice.[244] RCS customers whose

[237] 18 U.S.C. §2703(a).

[238] 18 U.S.C. §2703(d). Some courts have held that this "reasonable grounds" standard is a less demanding standard than "probable cause." *See In re* Application of the United States, 620 F.3d 304, 313 (3d Cir. 2010) ("We also conclude that this [§2703(d)] standard is a lesser one than probable cause.").

[239] 18 U.S.C. §2705(a).

[240] 18 U.S.C. §2711(2).

[241] However, if some other service provided by the utility allows the data collected by a smart meter to be stored or manipulated for the benefit of the utility's customers, it is possible that this system would fall within the definition of an RCS.

[242] The SCA allows providers of an RCS to disclose stored communications with the consent of the subscriber of an RCS. 18 U.S.C. §2702(b)(3).

[243] 18 U.S.C. §2703(b)(1).

[244] 18 U.S.C. §2703(b)(1)(B).

communications have been disclosed in violation of the SCA may pursue a civil cause of action for equitable relief, reasonable attorneys' fees and costs, and damages equal to the loss and gain associated with the offense but not less than $1,000.[245]

The Computer Fraud and Abuse Act (CFAA)

The Computer Fraud and Abuse Act (CFAA) prohibits intentionally accessing and obtaining information from a computer used in or affecting interstate commerce, without authorization or in excess of a granted authorization.[246] The definition of a computer for purposes of the CFAA is "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" excluding "an automated typewriter or typesetter, a portable hand held calculator, or other similar device...."[247]

The servers on a utility's network would likely fall squarely within the definition of a computer under the CFAA. Similarly, smart meters themselves also appear to meet the definition of a computer, insofar as they store customers' energy usage data and also perform logical operations by routing transmissions across the utility's network. Additionally, in light of the significant role that energy utilities play in the modern economy, the smart meter network would also likely be considered to have an effect on interstate commerce, even if they operate entirely within one state. Therefore, intentionally gaining access to the utility's servers or smart meters to obtain customer data would likely constitute a violation of the CFAA if done without the utility's authorization or in excess of an authorization granted by the utility.

The criminal penalties for violating the unauthorized access provisions of the CFAA have a three tier sentencing structure. Simple violations are punished as misdemeanors, imprisonment for not more than one year and/or a fine of not more than $100,000 ($200,000 for organizations).[248] At the next level, cases in which: "(i) the offense was committed for purposes of commercial advantage or private financial gain; (ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or (iii) the value of the information obtained exceeds $5,000" may be punished by imprisonment for not more than five years and/or a fine of not more $250,000 ($500,000 for organizations).[249] The third tier is for repeat offenders whose punishment is increased to imprisonment of not more than 10 years and/or a fine of not more than $250,000 ($500,000 for organizations) for a second or subsequent conviction.[250]

[245] 18 U.S.C. §2707.

[246] 18 U.S.C. §1030(a)(2). For more detailed information on the CFAA, *see* CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle.

[247] 18 U.S.C. §1030(e)(1).

[248] 18 U.S.C. §1030(c)(2)(A).

[249] 18 U.S.C. §1030(c)(2)(B).

[250] 18 U.S.C. §§1030(c), 3571.

The Federal Trade Commission Act (FTC Act)

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce"[251] and gives the Federal Trade Commission (FTC) jurisdiction to bring enforcement actions against "persons, partnerships, or corporations" that engage in these practices.[252] In the past, the FTC has used its authority under Section 5 to take action against businesses that violate their own privacy policies or that fail to adequately safeguard a consumer's personal information.[253] Although there do not appear to be any cases in which the FTC has taken action against an electric utility for failing to protect consumer smart meter data, the Commission would have authority to enforce Section 5 against a utility that fell within its statutory jurisdiction.

Covered Electric Utilities

This section considers whether the FTC would have Section 5 jurisdiction over each of the four types of electric utilities identified by the Energy Information Administration (EIA): investor-owned, publicly owned, federally owned, and cooperative.[254] It finds that the FTC clearly has jurisdiction over investor-owned utilities. It is unclear whether the Commission has jurisdiction over publicly owned utilities or federally owned utilities. The FTC could enforce Section 5 against for-profit electric cooperatives, and case law suggests that nonprofit electric cooperatives may also be subject to the act's requirements.

The FTC has jurisdiction to enforce Section 5 against "persons, partnerships, or corporations," with exceptions not applicable here.[255] Utilities that are "persons" or "partnerships" would be subject to the FTC's enforcement powers automatically,[256] as the statute does not provide any additional jurisdictional requirements for these entities. Most electric utilities, however, are organized as legal entities that would potentially fit within the definition of "corporation." The FTC Act states that, for the purposes of Section 5, the term "corporation":

> shall be deemed to include any company, trust, so-called Massachusetts trust, or association, incorporated or unincorporated, which is organized to carry on business for its own profit or that of its members, and has shares of capital or capital stock or certificates of interest, and any company, trust, so-called Massachusetts trust, or association, incorporated or unincorporated, without shares of capital or capital stock or certificates of interest, except partnerships, which is organized to carry on business for its own profit or that of its members.[257]

---

[251] 15 U.S.C. §45(a)(1).

[252] 15 U.S.C. §45(a)(2).

[253] *See* "Enforcement of Data Privacy and Security," *infra* p. 41; *see also* NIST PRIVACY REPORT, *supra* note 11, at 23 n.48.

[254] ENERGY INFO. ADMIN., ELECTRIC POWER INDUSTRY OVERVIEW (2007) [hereinafter EIA ELECTRIC POWER OVERVIEW], *available at* http://www.eia.gov/cneaf/electricity/page/prim2/toc2.html.

[255] 15 U.S.C. §45(a)(2).

[256] The FTC Act does not further define "persons" or "partnerships" or impose any additional jurisdictional requirements on these entities in the way that it does for "corporations." *See* 15 U.S.C. §44.

[257] 15 U.S.C. §44.

This definition, particularly in its use of the words "shall be deemed to include," suggests that a wide variety of legal entities could potentially constitute "corporations." Moreover, in *California Dental Ass'n v. FTC*, the Supreme Court remarked that the "FTC Act directs the Commission to prevent the *broad set of entities* under its jurisdiction" from violating Section 5.[258] In that case, the Court found that the term "corporation" also included *nonprofit* entities, so long as they imparted significant economic benefit to their members.[259] Thus, as the Court's opinion demonstrates, the key question when determining whether an entity is a "corporation" for the purposes of Section 5 jurisdiction is not what legal form the entity takes, but rather whether the entity is "organized to carry on business for its own profit or that of its members."

Investor-Owned Utilities

Investor-owned utilities are clearly subject to the FTC's Section 5 jurisdiction as "corporations." The EIA defines investor-owned electric utilities as those that "have the fundamental objective of producing a profit for their investors" and distributing these profits as dividends or reinvesting them in the business.[260] These utilities satisfy the definition of "corporation" under the statute because they are companies organized to carry on business for the profit of their investors.[261]

Publicly Owned Utilities

It is unclear whether the FTC has Section 5 jurisdiction over publicly owned utilities. The agency probably lacks jurisdiction over these utilities if it characterizes them as "corporations," but it is possible that it may have jurisdiction over them if it characterizes them as "persons." Publicly owned utilities include "municipals, public utility districts and public power districts, State authorities, irrigation districts, and joint municipal action agencies."[262] The EIA describes these as "nonprofit government entities that are organized at either the local or State level," are exempt from state and federal income taxes, and "provide service to their communities and nearby consumers at cost."[263] In contrast to investor-owned utilities or cooperatively owned utilities, publicly owned utilities obtain capital by issuing debt rather than selling an ownership interest in the utility to investors or members.[264]

As "Corporations"

Publicly owned utilities probably do not fall within the FTC's Section 5 jurisdiction over "corporations" because they are not organized to carry on business for profit. Rather, governments form these utilities for the sole purpose of distributing electricity to consumers at

[258] Cal. Dental Ass'n v. FTC, 526 U.S. 756, 768 (1999) (emphasis added) (internal quotation marks omitted).

[259] *Id.* at 766-69.

[260] EIA ELECTRIC POWER OVERVIEW, *supra* note 254.

[261] Indeed, the FTC has asserted Section 5 jurisdiction over holding companies with investor-owned electric utility subsidiaries in the past. *See, e.g., DTE Energy Co.*, 131 F.T.C. 962 (May 15, 2001) (complaint); *CMS Energy Corp.*, 127 F.T.C. 827 (June 2, 1999) (complaint). *See also In re* DTE Energy Co., FTC File No. 001 0067 (May 15, 2001) (consent order); *In re* CMS Energy Corp., FTC File No. 991 0046 (June 2, 1999) (consent order).

[262] EIA ELECTRIC POWER OVERVIEW, *supra* note 254.

[263] *Id.*

[264] DAVID E. MCNABB, PUBLIC UTILITIES: MANAGEMENT CHALLENGES FOR THE 21ST CENTURY 165 (2005).

cost.[265] Significantly, when publicly owned utilities realize net income—that is, revenues they earn in excess of their expenses—they either (1) use it to finance their operations in lieu of issuing more debt,[266] or (2) transfer it to the general fund of the political subdivision that they serve.[267] These utilities typically lack investors or members to which they could distribute net income as dividends.[268] Thus, publicly owned utilities are probably not "organized to carry on business" for profit and are probably exempt from the FTC's Section 5 jurisdiction if characterized as "corporations."

As "Persons"

It is unclear whether a court would find that the FTC has Section 5 jurisdiction over publicly owned utilities as "persons," as a court could employ several different canons of statutory interpretation when deciding whether "persons" includes state or local government entities.[269] In the 1980s, the FTC attempted to assert Section 5 jurisdiction over two state-chartered municipal corporations—the cities of New Orleans and Minneapolis—as "persons," alleging that the cities engaged in unfair methods of competition by assisting taxicab companies in maintaining high prices and stifling competition.[270] The Commission later withdrew both complaints, and thus no court considered whether jurisdiction was proper. More recently, the Commission has asserted jurisdiction over state government agencies that regulate certain professions such as dentistry,[271] optometry,[272] and funeral services.[273]

There appears to be only one court case that engages in a full discussion and interpretation of the meaning of "persons" under Section 5. In *California State Board of Optometry v. FTC*, the D.C. Circuit Court of Appeals considered "whether a State acting in its sovereign capacity is a 'person' within the FTC's enforcement jurisdiction."[274] The FTC had issued a rule declaring "certain state laws restricting the practice of optometry to be unfair acts or practices."[275] Petitioners, which were state boards of optometry and professional associations, argued that the court should strike down the rule because it went beyond the FTC's statutory authority.[276] In vacating the rule, the court found nothing in the relevant provisions of the FTC Act "to indicate that Congress intended to authorize the FTC to reach the 'acts or practices' of States acting in their sovereign capacities."[277]

---

[265] EIA ELECTRIC POWER OVERVIEW, *supra* note 254.

[266] MCNABB, *supra* note 264, at 165.

[267] EIA ELECTRIC POWER OVERVIEW, *supra* note 254.

[268] MCNABB, *supra* note 264, at 165.

[269] In contrast to entities that are "corporations," the FTC does not have to show that entities qualifying as "persons" are organized for profit. *See* 15 U.S.C. §44.

[270] *In re* City of Minneapolis, 105 F.T.C. 304 (May 7, 1985) (order withdrawing complaint); *In re* City of New Orleans, 105 F.T.C. 1 (Jan. 3, 1985) (order withdrawing complaint).

[271] *In re* N.C. State Bd. of Dental Exam'rs, 151 F.T.C. 607 (Feb. 3, 2011) (state action opinion); *In re* South Carolina State Bd. of Dentistry, 138 F.T.C. 229 (Sept. 12, 2003) (complaint).

[272] *In re* Mass. Board of Registration in Optometry, 110 F.T.C. 549 (June 13, 1988) (decision).

[273] *In re* Va. Bd. of Funeral Dirs. & Embalmers, 138 F.T.C. 645 (Oct. 1, 2004) (complaint).

[274] 910 F.2d 976, 979 (D.C. Cir. 1990).

[275] *Id.* at 978.

[276] *Id.* at 978-79.

[277] *Id.* at 980, 982.

A court approaching the question of whether "persons" includes publicly owned utilities would start with the language of the statute. Courts traditionally give broad deference to an agency when the agency interprets the extent of its own jurisdiction unless the reach of its jurisdiction is clear from reading the statute "under ordinary principles of construction."[278] Attempting to discern the Commission's jurisdiction under Section 5 of the FTC Act is difficult, as the statute does not define the term "persons" for the purposes of that provision. Title 1, Section 1 of the United States Code (the Dictionary Act) provides: "In determining the meaning of any Act of Congress, *unless the context indicates otherwise* ... the words 'person' and 'whoever' include corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals."[279]

However, the context in which "persons" appears in Section 5 probably forecloses the use of the default definition of "person" in the Dictionary Act. In Section 5, Congress listed the terms "persons," "partnerships," and "corporations" separately, which indicates that it intended to give each term independent significance. The terms "corporations" and "partnerships" would not have independent meaning in Section 5 if the term "persons" in Section 5 included the entities listed in the Dictionary Act. Furthermore, the FTC Act requires that "corporations" be organized for their own profit or the profit of their members in order for the FTC to exercise jurisdiction over them—a requirement it does not impose on the other entities.[280] By reading the term "persons" to include the entities listed in the Dictionary Act, the FTC could evade this additional requirement simply by bringing its complaint against an entity as a "person" rather than a "corporation"—a result that Congress probably did not intend. Thus, a court that ended its analysis here could find that the meaning of "persons" remains ambiguous. The court could then choose to defer to the FTC's broad interpretation of its own jurisdiction under the Supreme Court's decision in *Chevron U.S.A., Inc. v. NRDC, Inc.*[281]

The *California Optometry* court, however, declined to defer to the FTC's interpretation of its own jurisdiction because it found that principles of federalism outweighed *Chevron* deference.[282] Quoting the Supreme Court's decision in *Will v. Michigan Department of State Police*,[283] the

---

[278] *See* Cal. Dental Ass'n v. FTC, 526 U.S. 756, 765-66 (1999) ("Respondent urges deference to this interpretation of the Commission's jurisdiction as reasonable. But we have no occasion to review the call for deference here, the interpretation urged in respondent's brief being clearly the better reading of the statute under ordinary principles of construction.") (internal citations omitted); *see also* Chevron U.S.A., Inc. v. NRDC, Inc., 467 U.S. 837, 842-43 (1984).

[279] 1 U.S.C. §1 (emphasis added).

[280] *See* 15 U.S.C. §44.

[281] *Chevron*, 467 U.S. at 842-43. In that case, the Court held that

> When a court reviews an agency's construction of the statute which it administers, it is confronted with two questions. First, always, is the question whether Congress has directly spoken to the precise question at issue. If the intent of Congress is clear, that is the end of the matter; for the court, as well as the agency, must give effect to the unambiguously expressed intent of Congress. If, however, the court determines Congress has not directly addressed the precise question at issue, the court does not simply impose its own construction on the statute, as would be necessary in the absence of an administrative interpretation. Rather, if the statute is silent or ambiguous with respect to the specific issue, the question for the court is whether the agency's answer is based on a permissible construction of the statute. *Id.*

[282] Todd H. Cohen, *Double Vision: The FTC, State Regulation, and Deciding What's Best for Consumers*, 59 GEO. WASH. L. REV. 1249, 1267 (1991) ("In sum, the *California State Board of Optometry* court relied on federalism principles to justify protecting state interests. The court extended the judicially-created *Parker* state action doctrine to cover FTC trade regulation rules and applied the clear statement doctrine to prevent the FTC from invalidating a state law as unfair without additional congressional action.").

[283] 491 U.S. 58 (1989).

California Optometry court stated that "in common usage, the term person does not include the sovereign, and statutes employing the word are ordinarily construed to exclude it."[284] In the *Will* case, the Court considered whether the term "person" as it appeared in 42 U.S.C. §1983 included a state.[285] The Court held that it did not, invoking the principles of federalism when it wrote that "[t]his approach is particularly applicable where it is claimed that Congress has subjected the States to liability to which they had not been subject before."[286] The Court found that the statute's language fell "far short of satisfying the ordinary rule of statutory construction that if Congress intends to alter the 'usual constitutional balance between the States and Federal Government,' it must make its intention to do so 'unmistakably clear in the language of the statute.'"[287]

The Court's decision in *Will*, as interpreted by the D.C. Circuit in *California Optometry*, suggests that Congress must clearly indicate in a particular statute when it wishes to subject states to a new form of liability, particularly when this would change the balance between state and federal authority by intruding on the actions a state takes in its sovereign capacity. There does not appear to be a clear indication that Congress intended the word "persons" in the FTC Act to subject publicly owned utilities to FTC enforcement actions.[288] Thus, if the FTC's enforcement of Section 5 against a publicly owned utility would alter the balance between the state and federal governments, a court might read "persons" to exclude these utilities. As the *California Optometry* court indicated, whether the balance is altered may depend on whether the operation of the utility amounts to the state acting in its sovereign capacity (balance altered) or merely engaging in a proprietary function (balance not altered).[289] The *California Optometry* court suggested that whether a state is acting in its sovereign capacity or engaging in a proprietary function may vary according to the antitrust laws' state action doctrine, a multi-pronged analysis that is beyond the scope of this report.[290] If a court found that the state was acting in its sovereign capacity when the state (or one of its subdivisions) operated an electric utility, the court could hold that the FTC does not have Section 5 jurisdiction because of the federalism principles and clear statement rule that guided the interpretation of the statute in *Will* and were adopted by the court in *California Optometry*.[291]

A third possible choice for a court would be to adopt the reasoning of the FTC and find that Congress clearly intended "persons" to include government entities, because under the other antitrust laws, the term "persons" includes state and local government entities, and the antitrust

---

[284] *California Optometry*, 910 F.2d 976, 980 (D.C. Cir. 1990) (internal quotation marks omitted).

[285] *Will*, 491 U.S. at 60.

[286] *Id.* at 64.

[287] *Id.* at 65 (citations omitted).

[288] Representative Covington, the sponsor of the act, explained during floor debate on the measure that Section 5 "embraces within the scope of that section every kind of person, natural or artificial, who may be engaged in interstate commerce."51 CONG. REC. 14,928 (1914). Despite this remark, courts have not taken such a broad view of the FTC's jurisdiction under the act. Even the Supreme Court has held that there are some limits on the entities covered by Section 5. *See* Cal. Dental Ass'n v. FTC, 526 U.S. 756, 766-67 (1999) (requiring, for jurisdiction, that a "proximate relation" must exist between the activities of a nonprofit and the benefit it provides to its members, and implying that the activities must confer "more than *de minimis* or merely presumed economic benefits" on the members).

[289] *See California Optometry*, 910 F.2d at 980-81 ("This rule of statutory construction serves to ensure that the States' sovereignty interests are adequately protected by the political process.").

[290] *Id.* at 980. For more information on the factors that courts consider when making this determination, see FED. TRADE COMM'N, REPORT OF THE STATE ACTION TASK FORCE (2003), *available at* http://www.ftc.gov/os/2003/09/stateactionreport.pdf.

[291] *See* Cohen, *supra* note 282, at 1267.

laws, including the FTC Act,[292] should be read together.[293] The *California Optometry* court acknowledged this argument, writing that "several Supreme Court decisions hold that a State *is* a person for purposes of the antitrust laws."[294] The court ultimately rejected the argument, however, because it found that "when a State acts in a sovereign rather than a proprietary capacity, it is exempt from the antitrust laws even though those actions may restrain trade," and that this state action doctrine may "limit the reach of the FTC's enforcement jurisdiction."[295] Thus, if a court found that a state acted in its *proprietary* capacity when the state (or one of its subdivisions) operated a public utility, then the state action doctrine would not apply, and it would be possible for a court to find jurisdiction even under the *California Optometry* case. The FTC has advanced this reasoning, arguing that the state boards over which it asserts jurisdiction do not amount to the states acting in their sovereign capacities.[296] Whether the operation of a particular publicly owned utility consists of the state acting in its sovereign capacity or engaging in a proprietary function may vary according to the antitrust laws' state action doctrine, a multi-pronged analysis that is beyond the scope of this report.[297]

Thus, whether a court would find that the word "persons" in Section 5 includes certain government entities such as publicly owned utilities is unclear because it may depend on which, if any, of several principles of statutory construction the court adopts. A court could, among other options: (1) find that the meaning of "persons" in Section 5 is ambiguous, and thus defer to the FTC's broad interpretation of its own jurisdiction because of the *Chevron* doctrine; (2) find that the statute is ambiguous, but that principles of federalism outweigh the court's usual *Chevron* deference to the Commission's interpretation of its own jurisdiction—a determination that may require a court to find that the state is acting in its sovereign capacity when the state (or one of its subdivisions) operates an electric utility; or (3) find that Congress clearly intended "persons" to include government entities because Section 5 should be read together with the other antitrust laws, under which the term "person" includes state and local government entities—a determination that may require a court to find that the state is performing a proprietary function when the state (or one of its subdivisions) operates a utility.

Federally Owned Utilities

It is unclear whether the FTC could enforce Section 5 against a federally owned utility. Indeed, there does not appear to be any case in which the FTC has sought to enforce Section 5 against a federal agency.[298] The FTC probably lacks Section 5 jurisdiction over the nine federally owned

[292] Although this report focuses on the FTC's consumer law cases under Section 5 ("unfair or deceptive acts or practices"), and not its antitrust cases ("unfair methods of competition"), both types of prohibited activities share the same phrase for the purposes of determining the agency's jurisdiction: "persons, partnerships, or corporations." *See* 15 U.S.C. §45(a)(2).

[293] *See In re* Mass. Board of Registration in Optometry, 110 F.T.C. 549 (June 13, 1988) (decision) (citations omitted).

[294] *California Optometry*, 910 F.2d at 980 (citations omitted).

[295] *Id.* at 980 (citation omitted).

[296] *See, e.g.*, *In re* N.C. State Bd. of Dental Exam'rs, 151 F.T.C. 607 (Feb. 3, 2011) (state action opinion); *In re* Mass. Board of Registration in Optometry, 110 F.T.C. 549 (June 13, 1988) (decision).

[297] For more information on the factors that courts consider when making this determination, see FED. TRADE COMM'N, REPORT OF THE STATE ACTION TASK FORCE (2003), *available at* http://www.ftc.gov/os/2003/09/stateactionreport.pdf.

[298] This report does not consider whether any constitutional implications would result if the FTC, an independent executive branch agency, brought an enforcement proceeding against another executive branch agency. *See generally* Michael Eric Herz, *When Can the Federal Government Sue Itself?*, 32 WM. & MARY L. REV. 893 (1991).

utilities operating in the United States[299] if it characterizes them as "corporations." Like publicly owned utilities, federally owned utilities are not organized for profit. As the EIA notes, "federal power is not sold for profit, but to recover the costs of operations and repay the Treasury for funds borrowed to construct generation and transmission facilities."[300] If the Commission characterizes these utilities as "persons," it is unclear whether a court would find that this term includes government entities.[301]

As a practical matter, FTC enforcement of Section 5 against federally owned utilities is probably unnecessary in the context of smart meter data because of other federal laws, such as the Privacy Act,[302] that would likely protect this data when it is stored in records systems maintained by federal agencies, including federally owned utilities.[303]

Cooperatively Owned Utilities

For-profit electric cooperatives would clearly fall within the Commission's Section 5 jurisdiction over "corporations" operated for their own profit or that of their members.[304] Indeed, the FTC has maintained jurisdiction over for-profit cooperatives as "corporations" in the past, including a rural healthcare cooperative[305] and a wine maker.[306] However, it appears that most electric cooperatives—and particularly the cooperatives that will receive funds under the Department of Energy's Smart Grid Investment Grant program—are nonprofits.[307]

It is possible that the FTC would have Section 5 jurisdiction over these nonprofit electric cooperatives as "corporations" organized for profit. These distribution utilities are owned by the "consumers they serve," and those that are tax-exempt must "provide electric service to their members at cost, as that term is defined by the Internal Revenue Service."[308] However, when the activities of a cooperative result in revenues that exceed the cooperative's costs, these "net margins ... are considered a contribution of equity by the members that are required to be returned to the members consistent with the organization's bylaws and lender limitations imposed as a condition of loans."[309] Thus, in contrast to publicly owned utilities, which typically transfer any net income to the general fund of the government that they serve, electric cooperatives return net margins to their members as equity, and when that equity is retired by the board of directors, members receive cash payments.[310] Although it does not appear that a court has considered

---

[299] EIA ELECTRIC POWER OVERVIEW, *supra* note 254. Among these utilities are the Tennessee Valley Authority, the four power marketing administrations in the Department of Energy, and the Army Corps of Engineers. *Id.*

[300] *Id.*

[301] *See supra* notes 269-97 and accompanying text.

[302] 5 U.S.C. §552a.

[303] *See* "The Federal Privacy Act of 1974," *infra* p. 45.

[304] 15 U.S.C. §44.

[305] *In re* Minn. Rural Health Coop., FTC File No. 051 0199 (Dec. 28, 2010) (decision and order).

[306] *In re* Heublein, Inc., 96 F.T.C. 385 (Oct. 7, 1980) (final order).

[307] *See* DEP'T OF ENERGY, CASE STUDY – NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION SMART GRID INVESTMENT GRANT 1, *available at* http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NRECA_case_study.pdf.

[308] EIA ELECTRIC POWER OVERVIEW, *supra* note 254.

[309] *Id.* "Net margins" is the term given to "revenues in excess of the cost of providing service." *Id.*

[310] *See, e.g.*, Cent. Rural Electric Coop., Patronage Capital, http://www.crec.coop/CRECAdvantage/PatronageCapital/tabid/711/Default.aspx ("Allocated patronage capital appears as an entry on the permanent financial records of the (continued...)

whether the FTC has Section 5 jurisdiction over a nonprofit electric cooperative that returns its net margins to its consumer-members in addition to providing them with electricity service, the Supreme Court, as well as lower federal courts, have issued guidance on factors that a court may consider in answering this question.

Applicable Law

Under Section 5, the FTC Act requires that a "corporation" be "organized to carry on business for its own profit *or that of its members*."[311] In *California Dental Ass'n v. FTC*, the Court considered whether the FTC could enforce Section 5 against a "voluntary nonprofit association of local dental societies" that was exempt from paying federal income tax and furnished its members with "advantageous insurance and preferential financing arrangements" in addition to lobbying, litigating, and advertising on their behalf.[312] The Court found that the FTC had jurisdiction over the California Dental Association as a "corporation," stating that

> the FTC Act is at pains to include not only an entity "organized to carry on business for its own profit," but also one that carries on business for the profit "of its members." While such a supportive organization may be devoted to helping its members in ways beyond immediate enhancement of profit, no one here has claimed that such an entity must devote itself single-mindedly to the profit of others. It could, indeed, hardly be supposed that Congress intended such a restricted notion of covered supporting organizations, with the opportunity this would bring with it for avoiding jurisdiction where the purposes of the FTC Act would obviously call for asserting it.[313]

The Court declined to specify the percentage of a nonprofit entity's activities that must be "aimed at its members' pecuniary benefit" to subject it to FTC jurisdiction.[314] However, the Court wrote that a "proximate relation" must exist between the activities of the entity and the profits of its members, and implied that the activities must confer "more than *de minimis* or merely presumed economic benefits" on the members.[315] The Court's justification for this result was that "nonprofit entities organized on behalf of for-profit members have the same capacity and derivatively, at

---

(...continued)

cooperative and reflect [sic] your equity or ownership in CREC. When patronage capital is retired, a check or bill credit is issued to you and your equity in the cooperative is reduced. ... When considering a retirement, the board analyzes the financial health of the cooperative and will not authorize a retirement that will adversely affect the financial integrity of the cooperative."); Fall River Rural Electric Coop., Patronage Capital, http://www.frrec.com/myAccount/patronageCapital.aspx ("The Cooperative's Board of Directors retires patronage capital when finances allow, often on an annual basis. The oldest patronage capital is retired first. Fall River currently retires patronage capital on a rotation of approximately 20 years."); Kauai Island Util. Coop., Member Patronage Capital Information, http://www.kiuc.coop/member_patcap-qa.htm ("A portion of Patronage Capital may be periodically paid to the members upon approval of the Board of Directors and our lenders."); Sulphur Springs Valley Electric Coop., Inc., Patronage Capital Credits, http://www.ssvec.org/?page_id=583 ("Capital credits represent your share of the Cooperative's margins – margins are the operating revenue remaining after operating expenses. The amount assigned in your name depends on your energy purchases. To calculate this, we divide your annual energy purchase by the Cooperative's operating income for the year. The more electricity you buy, the more capital credits you earn.").

[311] 15 U.S.C. §44 (emphasis added).

[312] 526 U.S. 756, 759-60, 767 (1999).

[313] *Id.* at 766 (internal citations omitted).

[314] *Id.*

[315] *Id.* at 766-67.

least, the same incentives as for-profit organizations to engage in unfair methods of competition or unfair and deceptive acts."[316]

It is clear that the FTC may still have Section 5 jurisdiction even when the benefits that a nonprofit provides to its members are secondary to its charitable functions. In *American Medical Ass'n v. FTC*, the Second Circuit considered whether the FTC could enforce Section 5 against three medical professional associations, including the American Medical Association (AMA), a nonprofit corporation composed of "physicians, osteopaths, and medical students."[317] The court, acknowledging that the associations served "both the business and non-business interests of their member physicians," found jurisdiction because the "business aspects" of their activities, including lobbying for members and offering business advice to them, subjected them to the FTC's jurisdiction despite the fact that the business aspects "were considered secondary to the charitable and social aspects of their work."[318]

When determining whether jurisdiction exists, a court may consider other factors in addition to the benefits that the nonprofit provides to its members. In *Community Blood Bank v. FTC*, the Eighth Circuit considered whether a "corporation" included all nonprofit corporations.[319] The appeals court held that the FTC lacked Section 5 jurisdiction over nonprofit blood banks because the banks' activities did not result in "profit" in the sense of "gain from business or investment over and above expenditures."[320] The blood banks, the court observed, lacked shares of capital, capital stock, or certificates, and were "organized for and actually engaged in business for only charitable purposes."[321] One bank's articles of incorporation touted the entity's charitable purposes, and all of the banks were exempt from paying federal income taxes.[322] Upon dissolution, the corporations would transfer their assets to other charitable or nonprofit organizations.[323] In addition, none of the funds collected by the blood banks had "ever been distributed or inured to the benefit of any of their members, directors or officers."[324] The court found that these factors made the blood banks "charitable organizations" both "in law and in fact," exempting them from the FTC's Section 5 jurisdiction.[325]

Analysis

The case law suggests several factors that a court may weigh when determining whether a private, nonprofit entity composed of members, such as an electric cooperative, is subject to the FTC's Section 5 jurisdiction as a "corporation."[326] The most significant factor is whether the nonprofit

[316] *Id.* at 768.

[317] 638 F.2d 443, 446 (1980).

[318] *Id.* at 448. The court noted in passing that the AMA's articles of incorporation stated that one purpose of the organization was to "safeguard the material interests of the medical profession." *Id.*

[319] 405 F.2d 1011, 1015 (8th Cir. 1969).

[320] *See id.* at 1017. The court also remarked that at least one case had established that "even though a corporation's income exceeds its disbursements its nonprofit character is not necessarily destroyed." *Id.*

[321] *Id.* at 1020, 1022.

[322] *Id.* at 1020.

[323] *Id.*

[324] *Id.*

[325] *Id.* at 1019.

[326] This analysis assumes that a court would extend the holdings of the applicable case law, which covered entities organized as nonprofit corporations and professional associations, to include entities organized as nonprofit electric (continued...)

provides an economic benefit to its members that is more than *de minimis* and that is proximately related to the nonprofit's activities. This benefit need not be the sole—or even primary—function of the nonprofit. Additional factors that the case law suggests weigh in favor of a finding of jurisdiction include that the nonprofit: (1) has gain from its business or investments that exceeds its expenditures; (2) has shares of capital or capital stock or certificates; (3) is not organized solely for charitable purposes or does not engage only in charitable work; (4) has articles of incorporation that list profit-seeking objectives; (5) is subject to federal income tax liability; (6) would distribute its assets to profit-seeking entities upon dissolution; and (7) distributes any of the funds it collects to its members, directors, or officers.

It is possible that the FTC has Section 5 jurisdiction over nonprofit electric cooperatives, although the outcome in any particular case may depend on the characteristics of the individual utility. A court could find that the typical nonprofit electric cooperative provides "economic benefit" to its members in at least two ways: (a) by providing electricity service to members;[327] and (b) by returning net margins to members in the form of patronage capital, which is an ownership interest in the cooperative that is later converted to cash payments to members when that capital is retired.[328] With regard to (a), it is likely that a court would find that electricity service is an "economic benefit" as defined in the case law. In *California Dental Ass'n*, the nonprofit professional association provided "advantageous insurance and preferential financing arrangements," as well as lobbying, litigation, and advertising services to its members.[329] In *American Medical Ass'n*, the nonprofit lobbied on behalf of its members and offered business advice to members.[330] These benefits, it is assumed, enabled the members to more easily conduct business profitably. Electricity service allows people to conduct activities at all times of the day, and thus provides a similar and clearly significant economic benefit to those who use it, whether for business or recreational purposes. As the primary objective of an electric cooperative is to provide electricity service to members, the necessary proximate relation between the activities of the nonprofit and the benefit to its members clearly exists.

Despite its pecuniary nature, there are a few problems with considering benefit (b), patronage capital, to be an "economic benefit" as defined by the Court. First, it is not clear that patronage capital actually is a benefit. A court could view patronage capital as a no-interest *loan* from the consumer-member to the utility,[331] or, because it is typically allocated to member accounts in a manner proportional to members' spending on electricity, simply a *refund* of money collected from the members that reflects the actual cost of providing service in a particular year.[332] If

---

(...continued)

cooperatives.

[327] Many cooperatives provide other services to their communities that could constitute "economic benefits." The National Rural Electric Cooperative Association notes that, "In addition to electric service, many electric co-ops are involved in community development and revitalization projects" that include "small business development and jobs creation, improvement of water and sewer systems, and assistance in delivery of health care and educational services." Nat'l Rural Electric Coop. Ass'n, Member Directory, http://www.nreca.coop/members/MemberDirectory/Pages/default.aspx.

[328] *See* sources cited *supra* note 310.

[329] Cal. Dental Ass'n v. FTC, 526 U.S. 756, 759-60, 767 (1999).

[330] Am. Med. Ass'n v. FTC, 638 F.2d 443, 448 (1980).

[331] *See, e.g.*, Cent. Rural Electric Coop., Patronage Capital, http://www.crec.coop/CRECAdvantage/PatronageCapital/tabid/711/Default.aspx ("These margins represent an interest-free loan of operating capital by the membership to the cooperative.").

[332] *See, e.g.*, Kauai Island Util. Coop., Member Patronage Capital Information, http://www.kiuc.coop/member_patcap-(continued...)

adopted by a court, neither of these characterizations would appear to be consistent with the "profit" that the statute describes[333] or the "economic benefit" that the Supreme Court requires for a nonprofit to be a "corporation."

Second, even if a court found patronage capital to be an economic benefit, it is not clear that it is more than *de minimis*. Patronage capital must be "retired" before members receive cash payments for it.[334] Retirements are made at the discretion of the cooperative's board of directors because the capital is needed to finance the cooperative's ongoing expenses, and thus retirement of a class of capital typically occurs after a long rotation period, such as 20 years.[335] Although the Supreme Court did not hold that an "economic benefit" must produce *immediate* advantage to the members of a nonprofit, a court could potentially view the decades-long delay in cash payments as significantly decreasing the degree of economic benefit that the capital provides. In addition, patronage capital would probably be considered *de minimis* if the cooperative's net margins were small, as this would mean that little capital would be issued to members. It is thus difficult to discern whether a court would find that an economic benefit accrues to members as a result of their receipt of patronage capital, which nevertheless probably bears the requisite "proximate relation" to the activities of the cooperative that produce any net margins distributed as capital.

With regard to the additional factors, those favoring jurisdiction include (2) cooperatives typically have shares of capital stock, including patronage capital;[336] (3) cooperatives do not operate solely for the benefit of the people outside of the organization like the nonprofits in *Community Blood Bank* did because cooperatives provide electricity service and patronage capital to their members;[337] and (7) an electric cooperative typically returns any net margins to members in the form of patronage capital, an ownership interest refunded to consumer-members as cash when the capital is retired.[338] Factors that cannot be evaluated because they are specific to each individual cooperative include (1) whether the revenues of the cooperative exceed its expenditures; (4) the particular objectives listed in a cooperative's articles of incorporation or other foundational document; (5) whether a nonprofit electric cooperative is exempt from federal income tax liability, which depends on whether it meets the requirements under Section 501(c)(12) of the Internal Revenue Code;[339] and (6) whether a cooperative would distribute its assets to profit-seeking entities upon dissolution—a factor that also may depend on state laws.[340]

It is likely that a court would find that nonprofit electric cooperatives impart economic benefits to their members by distributing electricity to them or, possibly, by issuing patronage capital to them. However, because many of the other factors that courts consider may differ for each

---

(...continued)

qa.htm (characterizing the retirement of patronage capital as a "refund").

[333] 15 U.S.C. §44.

[334] *See* sources cited *supra* note 310.

[335] *See id.*

[336] *See* Nat'l Rural Electric Coop. Ass'n, Seven Cooperative Principles, http://www.nreca.coop/members/SevenCoopPrinciples/Pages/default.aspx (describing "Members' Economic Participation").

[337] Whether electricity service and patronage capital, which are clearly benefits, constitute "economic benefits" within the meaning of the Supreme Court's holding in *California Dental Ass'n* is a separate question.

[338] *See* sources cited *supra* note 310.

[339] I.R.C. §501(c)(12).

[340] *See* Cmty. Blood Bank v. FTC, 405 F.2d 1011, 1020 (8th Cir. 1969).

particular cooperative, it is not possible to draw any general conclusions about whether the FTC would have Section 5 jurisdiction over these entities as "corporations."

Enforcement of Data Privacy and Security

If the FTC has Section 5 jurisdiction over a particular electric utility, it may bring an enforcement action against the utility if its privacy or security practices with regard to consumer smart meter data constitute "unfair or deceptive acts or practices in or affecting commerce."[341] The FTC Act defines an "unfair" act or practice as one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[342] According to the FTC, an act or practice is "deceptive" if it is a material "representation, omission or practice" that is likely to mislead a consumer acting reasonably in the circumstances.[343] The history of the Commission's enforcement of consumer data privacy and security practices shows that the agency has brought complaints against entities that (1) engage in "deceptive" acts or practices by failing to comply with their stated privacy policies; or (2) employ "unfair" practices by failing to adequately secure consumer data from unauthorized parties.[344] Often, conduct constituting a violation could fall under either category, as a failure to protect consumer data may be an unfair practice because of the unavoidable injury it causes, as well as a deceptive practice because it renders an entity's privacy policy materially misleading.

"Deceptive" Privacy Statements

A utility that fails to comply with its own privacy policy may engage in a "deceptive" act or practice under Section 5 of the FTC Act. In *Facebook, Inc.*, the FTC alleged, among other things, that the social networking site violated promises contained in its privacy policy when it made users' personal information accessible to third parties without users' consent.[345] Facebook had claimed that users could limit third-party access to their personal information on the site. Despite this promise, applications run by users' Facebook friends were able to access the users' personal information. The Commission also charged that Facebook altered its privacy practices without users' consent, causing personal information that had been restricted by users to be available to third parties. This change, which allegedly "caused harm to users, including, but not limited to, threats to their health and safety, and unauthorized revelation of their affiliations" constituted both a "deceptive" and an "unfair" practice in the view of the Commission.[346] Finally, the Commission alleged that Facebook had represented to users that it would not share their personal information with advertisers but had done so anyway.

---

[341] 15 U.S.C. §45(a)(1). For more details on FTC enforcement of consumer data privacy and security under Section 5, see CRS Report RL34120, *Federal Information Security and Data Breach Notification Laws*, by Gina Stevens.

[342] 15 U.S.C. §45(n).

[343] *In re* Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984) (policy statement at end of opinion).

[344] *See Consumer Privacy: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 11th Cong. (2010) (statement of Jon D. Leibowitz, Chairman, Fed. Trade Comm'n) (describing the FTC's enforcement activity in the areas of consumer data privacy and security), *available at* http://www.ftc.gov/os/testimony/100727consumerprivacy.pdf. The FTC recently released a preliminary report on the consumer privacy implications of new technologies. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[345] FTC File No. 092 3184 (Nov. 29, 2011) (complaint).

[346] *Id.*

In *Twitter, Inc.*, the FTC alleged that the social networking site engaged in "deceptive" acts when it violated claims made in its privacy policy about the security of consumer data by failing to "use reasonable and appropriate security measures to prevent unauthorized access to nonpublic user information."[347] The Commission found that Twitter had permitted its administrators to access the site with easy-to-guess passwords and failed to limit the extent of administrators' access according to the requirements of their jobs. In a consent order, the company agreed not to misrepresent its privacy controls and to implement a comprehensive information security program that would be assessed by an independent third party.[348]

As smart meter data becomes valuable to third parties,[349] utilities may be tempted to sell or share this information with others to increase revenues and provide new services to their customers. If prohibited by the terms of the utility's privacy policy, it may be a "deceptive" act or practice for the utility to share a consumer's personal information with third parties without a consumer's consent.[350] The FTC could also find deception when a utility represents that its privacy controls are capable of protecting smart meter data when, in fact, they are not.

"Unfair" Failure to Secure Consumer Data

Failure to Protect Against Common Technology Threats or Unauthorized Access

The FTC may consider it an "unfair" practice when an electric utility fails to safeguard smart meter data from well-known technology threats as the data travels across the utility's communications networks. For example, in *DSW Inc.*, the FTC brought enforcement proceedings against the respondent, the owner of several shoe stores.[351] The agency alleged that the respondent failed to protect customers' credit card and check information as it was transmitted to the issuing bank for authorization. The information collected at the register traveled wirelessly to the store's computer network, and from there to the bank or check processor, which communicated its response back to the store through the same channels. The agency charged that

> [a]mong other things, respondent (1) created unnecessary risks to the information by storing it in multiple files when it no longer had a business need to keep the information; (2) did not use readily available security measures to limit access to its computer networks through wireless access points on the networks; (3) stored the information in unencrypted files that could be accessed easily by using a commonly known user ID and password; (4) did not limit sufficiently the ability of computers on one in-store network to connect to computers on other in-store and corporate networks; and (5) failed to employ sufficient measures to detect unauthorized access. As a result, a hacker could use the wireless access points on one in-store computer network to connect to, and access personal information, on the other in-store and corporate networks.[352]

[347] FTC File No. 092 3093 (Mar. 2, 2011) (complaint).

[348] FTC File No. 092 3093 (Mar. 2, 2011) (decision and order)

[349] NIST PRIVACY REPORT, *supra* note 11, at 14, 35-36.

[350] As suggested below, it may also be an "unfair" practice, regardless of whether the utility has a privacy policy.

[351] FTC File No. 052 3096 (Mar. 7, 2006) (complaint).

[352] *Id.*

Similarly, in *Cardsystems Solutions, Inc.*, the Commission brought a complaint against a credit and debit card authorization processor.[353] The FTC alleged that the respondent failed to protect its systems by neglecting to guard its network against "commonly known or reasonably foreseeable attacks" that could be avoided using low-cost methods.[354] As part of settlement agreements in *DSW* and *Cardsystems*, the respondents had to create "a comprehensive information security program" to protect consumer information that would be assessed periodically by an independent third party.[355]

Smart meters also transmit personal consumer information, often wirelessly, across several different communications networks located in various physical places.[356] Thus, it is possible that the FTC would view a utility's failure to protect smart meter data against common technology threats as an "unfair" practice if the utility could have avoided the threats by using low-cost methods such as encrypting the data; storing it in fewer places and for no longer than needed; implementing basic wireless network security; and taking other reasonable measures suggested by the agency in *DSW Inc.*

Failure to Dispose of Data Safely

A utility's failure to dispose of smart meter data safely may also constitute an "unfair" practice under Section 5. For example, in *Rite Aid Corp.*, the respondent, the owner of retail pharmacy stores, purportedly failed to safely dispose of personal information in its possession when it neglected to: "(1) implement policies and procedures to dispose securely of such information," including rendering "the information unreadable in the course of disposal; (2) adequately train employees to dispose securely of such information; (3) use reasonable measures to assess compliance with its established policies and procedures for the disposal of such information; and (4) employ a reasonable process for discovering and remedying risks to such information."[357] The information was later found in various publicly accessible garbage dumpsters in readable form. This suggests that utilities holding smart meter data and other personal information, whether on electronic or physical media, must ensure that the methods used to destroy this data render it unreadable to third parties.

Penalties

There is no private right of action in the FTC Act. If the Commission has "reason to believe" that a violation has occurred, it may, after notice to the respondent and an opportunity for a hearing, issue an order directing the respondent to cease and desist from acts or practices that the agency finds violate the act.[358] If the respondent disobeys an order that has become final, the U.S. Attorney General may bring an action in district court seeking the imposition of civil monetary

[353] FTC File No. 052 3148 (Sept. 5, 2006) (complaint).

[354] *Id.*

[355] *See, e.g.*, *In re* Cardsystems Solutions, Inc., FTC File No. 052 3148 (Sept. 5, 2006) (decision and order).

[356] NIST PRIVACY REPORT, *supra* note 11, at 23.

[357] FTC File No. 072 3121 (Nov. 12, 2010) (complaint).

[358] 15 U.S.C. §45(b). The Commission may seek a preliminary injunction in district court if it "has reason to believe" that an entity subject to the Commission's jurisdiction "is violating, or is about to violate, any provision of law enforced" by the FTC, and such an injunction would be in the public interest. 15 U.S.C. §53(b). In "proper cases the Commission may seek, and after proper proof, the court may issue, a permanent injunction." *Id.*

penalties of up to $16,000 per violation ($16,000 per day for continuing violations), as well as further injunctive and equitable relief that the court deems appropriate.[359]

After a party becomes subject to a final cease and desist order under the act, the Commission may seek redress for consumers by bringing suit in state or federal court against the party if the Commission "satisfies the court that the act or practice to which the cease and desist order relates is one which a reasonable man would have known under the circumstances was dishonest or fraudulent."[360] "Such relief may include, but shall not be limited to, rescission or reformation of contracts, the refund of money or return of property, the payment of damages," and public notification of the violation, "except nothing in [15 U.S.C. §57b(b)] is intended to authorize the imposition of any exemplary or punitive damages."[361] Once the Commission has issued a final cease and desist order (not a consent order) finding an act or practice to be deceptive, then it may bring suit in district court to obtain a civil penalty against an entity that engages in that act or practice: (1) after the order became final ("whether or not such person, partnership, or corporation was subject to such cease and desist order"); and (2) "with actual knowledge that such act or practice is unfair or deceptive and is unlawful" under Section 5 of the FTC Act.[362]

The Federal Privacy Act of 1974 (FPA)

Smart meter electricity usage data pertaining to U.S. citizens or permanent residents that is retrievable by personal identifier from a system of records maintained by any federal "agency," including federally owned utilities, is subject to the protections contained in the Privacy Act[363] when it is maintained, collected, used, or disseminated by the agency.

Federally Owned Utilities as "Agencies"

All nine of the federally owned utilities are federal agencies covered by the Privacy Act. For the purposes of the act, the term "agency" includes, but is not limited to, "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency."[364] According to EIA, utilities that are part of an executive department include the four power marketing administrations in the Department of Energy (Bonneville, Southeastern, Southwestern, and Western), the International Boundary and Water Commission in the Department of State, and the Bureau of Indian Affairs and the Bureau

[359] 15 U.S.C. §45(l). The size of the civil monetary penalty was last adjusted for inflation in 2009. 16 C.F.R. §1.98.

[360] 15 U.S.C. §57b(a)(2).

[361] 15 U.S.C. §57b(b).

[362] 15 U.S.C. §45(m)(1)(B).

[363] 5 U.S.C. §552a. The federally owned utilities primarily sell electricity to nonprofit electric utilities on the wholesale markets rather than distribute electricity directly to consumers. EIA ELECTRIC POWER OVERVIEW, *supra* note 254. As these utilities provide only about 1% of total sales of electricity to end user consumers, *id.*, they may be unlikely to acquire consumer smart meter data, which is typically transmitted to distribution utilities. However, as the smart grid becomes more interconnected, more utilities at different points in the smart grid may come into possession of this data. NIST PRIVACY REPORT, *supra* note 11, at 23.

[364] *See* 5 U.S.C. §552(f)(1). The act also covers data in a "system of records" operated by a government contractor on behalf of a federal agency. *See* 5 U.S.C. §552a(m).

of Reclamation in the Department of the Interior.[365] The U.S. Army Corps of Engineers resides in the Department of Defense, which is an executive department.[366] The Tennessee Valley Authority is a government-owned corporation.[367]

Smart Meter Data as a Protected "Record"

The Privacy Act protects the type of electricity usage data gathered by smart meters, provided that the data pertains to U.S. citizens or permanent residents, is personally identifiable, and is retrievable by the individual's name or another personal identifier. The Privacy Act "governs the collection, use, and dissemination of a 'record' about an 'individual' maintained by federal agencies in a 'system of records.'"[368] Under the statute, a "record" is "any item, collection, or grouping of information about an individual that is maintained by an agency ... that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."[369]

An "individual" is defined as "a citizen of the United States or an alien lawfully admitted for permanent residence."[370] A "system of records" is "a group of any records under the control of any agency from which information is retrieved by the name of the individual" or other personal identifier "assigned to the individual."[371]

Smart meter data held by an agency certainly fits within the broad definition of a "record" because it is a grouping of information about an individual, namely, data on that individual's electricity usage. The data is typically stored along with a consumer's account information, which usually includes a consumer's name, social security number, or other "identifying particular."[372] Thus, smart meter data would constitute a protected "record" under the Privacy Act, assuming that it pertains to a citizen of the United States or lawful permanent resident and is retrievable by a personal identifier such as a consumer's name or account number.

Requirements

For information on the general safeguards that the Privacy Act provides for data that is maintained by a federal agency and meets the other requirements for a covered record under the act, see CRS Report RL34120, *Federal Information Security and Data Breach Notification Laws*, by Gina Stevens.

---

[365] EIA ELECTRIC POWER OVERVIEW, *supra* note 254.

[366] DEP'T OF THE ARMY CORPS OF ENG'RS, CIVIL WORKS STRATEGIC PLAN 1 (2004), *available at* http://www.corpsresults.us/pdfs/cw_strat.pdf. It is also a "Major Command within the Army." *Id.*

[367] Tenn. Valley Auth., About TVA, http://www.tva.com/abouttva/index.htm.

[368] *See* CRS Report RL34120, *Federal Information Security and Data Breach Notification Laws*, by Gina Stevens (citations omitted).

[369] 5 U.S.C. §552(a)(4).

[370] 5 U.S.C. §552a(a)(2).

[371] 5 U.S.C. §552a(a)(5).

[372] NIST PRIVACY REPORT, *supra* note 11, at 26-27.

Author Contact Information

Brandon J. Murrill
Legislative Attorney
bmurrill@crs.loc.gov, 7-8440

Edward C. Liu
Legislative Attorney
eliu@crs.loc.gov, 7-9166

Richard M. Thompson II
Legislative Attorney
rthompson@crs.loc.gov, 7-8449

BEFORE THE PUBLIC UTILITIES COMMISSION OF THE

STATE OF CALIFORNIA

Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's Own Motion to Actively Guide Policy in California's Development of a Smart Grid System	Rulemaking 08-12-009 (Filed December 18, 2008)

JOINT COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY AND THE ELECTRONIC FRONTIER FOUNDATION ON PROPOSED POLICIES AND FINDINGS PERTAINING TO THE SMART GRID

JENNIFER LYNCH, Attorney[1]
Samuelson Law, Technology & Public Policy Clinic
University of California, Berkeley School of Law
396 Simon Hall
Berkeley, CA 94720-7200
(510) 642-7515
Attorney for CENTER FOR DEMOCRACY & TECHNOLOGY

LEE TIEN, Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333 x102
Attorney for ELECTRONIC FRONTIER FOUNDATION

Dated: March 9, 2010

[1] Berkeley Law students Jonas Herrell, David Marty, and Shane Witnov, along with School of Information Masters Candidate, Longhao Wang, participated in the drafting of these comments.

BEFORE THE PUBLIC UTILITIES COMMISSION OF THE

STATE OF CALIFORNIA

Order Instituting Rulemaking to Consider Smart Grid Technologies Pursuant to Federal Legislation and on the Commission's Own Motion to Actively Guide Policy in California's Development of a Smart Grid System	Rulemaking 08-12-009 (Filed December 18, 2008)

JOINT COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY AND THE ELECTRONIC FRONTIER FOUNDATION ON PROPOSED POLICIES AND FINDINGS PERTAINING TO THE SMART GRID

I. Introduction

The Center for Democracy & Technology ("CDT") and the Electronic Frontier Foundation ("EFF") file these joint comments in response to the Assigned Commissioner and Administrative Law Judge's Joint Ruling Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid, issued February 8, 2010 ("Joint Ruling"). CDT and EFF thank the Commission for the opportunity to submit comments discussing these important questions and commend the Commission's initiative on the matters to date.

The Center for Democracy & Technology is a non-profit, public interest organization with broad experience and expertise in matters of consumer privacy and emerging technologies. CDT has offices in Washington, DC and San Francisco, California. EFF is a non-profit member-supported organization based in San Francisco, California, that works to protect free speech and privacy rights in an age of increasingly sophisticated technology.

In addressing the issues raised by the Joint Ruling, we recommend the following:

- Privacy concerns raised by data collection within the Smart Grid require regulatory action on the part of the Commission. (*See Section II)*
- The Commission's authority to regulate consumer privacy and data access issues on the Smart Grid is derived from the California Constitution, Senate Bill 17, and the Commission's past decisions. (*See Section III*)
- The Commission should define the scope of customer energy data that warrants privacy protection. (*See Section IV)*
- The Commission should adopt privacy and security principles based on the Fair Information Practice principles (FIPs) to ensure that Smart Grid proposals will provide the privacy protections required by state and federal law. (*See Section V*)
- To fulfill the requirements of Senate Bill 17, the Commission should require utilities to employ Fair Information Practice principles as part of their Smart Grid deployment plans. (*See Section VI*)
- The Commission should consider and adopt our recommended modification to the Proposed Access Rule, as provided in our Appendix A. (*See Section VII*)
- The Commission should include privacy-related quantitative metrics for Smart Grid implementations. (*See Section VIII*)
- The Commission should not wait for privacy standards from the national standard setting bodies, and should adopt the Fair Information Practice principles now. (*See Section IX*)

We hope that our comments and recommendations here will both advance the Commission's understanding of the important privacy interests that are at stake in these proceedings and provide useful guidance to the Commission as it seeks compliance with the requirements and mandates of State Senate Bill 17, the Federal Energy Independence and Security Act of 2007, and the California Constitution.

II. Privacy Concerns Raised By Data Collection within the Smart Grid Require Regulatory Action on the Part of the Commission

A. Data Flows Enabled by Smart Grid Technology Represent a Profound Shift in the Customer-to-Utility Relationship

The Smart Grid promises great benefits to consumers and the environment, including lowered energy costs, increased usage of environmentally friendly power sources, and enhanced security against attack and outage. At the same time, however, the Smart Grid presents new privacy threats through its enhanced collection and transmission of detailed consumption data – data that can reveal intimate details about activities within the home and that can easily be transmitted from one party to another. The following aspects of these expanded data flows represent a profound shift from the traditional customer-to-utility relationship:

(1) Granularity of Usage Information: The Smart Grid entails collection of much more detailed data about consumer energy consumption than previous technologies allowed. Whereas historically a consumer's consumption data may have been collected once a month or less frequently from a traditional meter fixed to the side of a house, in the Smart Grid, sophisticated new systems will collect and record this data at much shorter time intervals—down to real-time or near real-time intervals. The emergence of increasingly sophisticated metering technologies is enabling the unprecedented collection of energy consumption data—from 750 to 3,000 (or more) data points a month— and will reveal variations in consumption that can reflect specific household activities such as sleep, work, and travel habits.[2]

(2) New Types of Information: Smart Grid technologies collect a much greater variety of information than has been collected by conventional energy services. In addition to detailed energy consumption data, utilities may collect distributed generation data, unique identifiers and functionality of home appliances, temperature inside the home, and location information of plug-in hybrid electric vehicles, just to name a few. And this is only the raw data. With this data in

[2] Jack I. Lerner & Deirdre K. Mulligan, *Taking the 'Long View' on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 Stan. Tech. L. Rev. 3. 3 (2008).

hand, it becomes trivial to infer presence and absence in the home, sleep schedules, and other highly personal routines.[3]

(3) Third Party Incentives and Access: The sheer volume of granular data provided by Smart Grid technologies, combined with its revealing nature, will make it highly attractive to a number of parties other than the utilities themselves, including marketers, law enforcement or other government actors, civil litigants, and criminals,[4] The attraction for marketers, for example, has already created an emerging market in consumer energy data. Within the new Smart Grid, third-party, non-utility operations will have unprecedented incentives to gain access to customer data. Beyond direct access to data held at utilities, third parties will seek to use utilities as conduits for customer information or will market devices that pull customer data directly from within the home, bypassing the utility's equipment.

The challenge for the Commission is to develop rules that both protect the consumer against misuse of this data and empower the consumer to access this data, use it and share it with entities other than the utility as they offer new and useful services to consumers.

B. New Technologies and Services Create Attendant Privacy Risks

New energy services that allow consumers access to their own detailed usage data present potential benefits in terms of energy efficiency and reliability. Yet these services will allow entities other than utilities to receive consumer energy consumption data and use it in new ways. This profound shift in the data flow away from the traditional consumer-to-utility relationship challenges key assumptions underlying existing privacy laws and regulations.

Further, the emergence of increasingly sophisticated metering technologies, which enable the unprecedented collection of energy consumption data, will remove a "latent structural limitation" that previously protected the revelation of intimate details about household activities.[5]

---

[3] Mikhail Lisovich, Deirdre Mulligan, & Stephen Wicker, *Inferring Personal Information from Demand-Response Systems*, IEEE Security & Privacy, Jan.-Feb. 2010, at 11-20.

[4] *See* § II.B, *infra*.

[5] *See* Harry Surden, *Structural Rights in Privacy*, 60 SMU L. Rev. 1605, 1626 (2007) (noting how "the widespread diffusion of an emerging technology effectively causes a rights-shift with respect to privacy interests protected by latent structural constraints.").

For example, new non-intrusive appliance load monitoring ("NALM") techniques make it easy to reconstruct information about energy consumption of individual appliances from a household's aggregate smart meter data,[6] and researchers have already compiled libraries of appliance load signatures.[7] Research shows that analyzing fifteen-minute interval aggregate household energy usage data can by itself pinpoint the use of most major home appliances.[8] As the time intervals between data collection points decrease, home appliance use will be inferable from overall utility usage data with greater and greater accuracy.[9]

Activities that might be revealed through analysis of home appliance use data include personal sleep and work habits, cooking and eating schedules, the presence of certain medical equipment and other specialized devices, presence or absence of persons in the home, and activities that might seem to signal illegal, or simply unorthodox, behavior.[10] As a result, information collected by the Smart Grid becomes highly valuable for many purposes other than energy efficiency, most prominently: commercial exploitation by advertisers and marketers, household surveillance by law enforcement, and access by criminals attempting to break into homes or commit identity theft.

1. Commercial Interests in Acquiring Customer Energy Data Create Privacy Risks

Because of the intimacy of home life, data collected by Smart Grid technologies and services could be used for purposes especially contrary to consumer interests and expectations. For example, an analysis of smart meter data revealing customers' home activities and daily routines could be commercially valuable to life insurance companies looking to adjust rates for customers with purportedly unhealthy lifestyles. Financial institutions making home mortgage loans might also be interested in their customers' energy usage records to verify whether the customers are actually living in those houses. Advertising companies offering behavioral

---

[6] Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies* app. A at A-1 (2009), *available at* http://ssrn.com/abstract=1462285.

[7] *Id.* at 2. The construction of load pattern libraries can be manually crafted, or generated by machine learning algorithms such as a neutral network.

[8] Research suggests this can be done with accuracy rates of over 90 percent. *See* Elias Leake Quinn, *Privacy and the New Energy Infrastructure* 28 (2009), *available at* http://ssrn.com/abstract=1370731.

[9] California utilities are already deploying smart meters that are capable of taking usage readings every five seconds. *See* Calif. Energy Comm'n, CEC-400-2008-027-CT, *Proposed Load Management Standards* 25 (Draft Comm. Report, 2008), *available at* http://www.energy.ca.gov/2008publications/CEC-400-2008-027/CEC-400-2008-027-CTD.PDF.

[10] Lerner & Mulligan, *supra* note 2.

targeting products might wish to enhance existing customer profiles with energy usage data that reveals customer activities and habits, following a recent trend in the merging of online and offline data sources to enhance targeted third-party advertising.[11]

2. Government Agency Incentives to Acquire Customer Energy Data Create Privacy Risks

The detailed and revealing nature of Smart Grid data also will be valuable for surveillance by government agencies. For example, law enforcement agencies already use electricity consumption data. In *Kyllo v. United States*,[12] the government relied on electrical utility records to develop its case against a suspected marijuana grower.[13] Government agents issued a subpoena to the suspect's utility to obtain energy usage records and then used a utility-prepared "guide for estimating appropriate power usage relative to square footage, type of heating and accessories, and the number of people who occupy the residence" to show that the suspect's power usage was "excessive" and thus "consistent with" a marijuana-growing operation.[14] In 2004, a California family was put under surveillance by law enforcement for having an unusually high electricity bill, which turned out to merely reflect the legitimate activities of a busy household.[15] In 2000, the California Narcotic Officers' Association unsuccessfully attempted to get the Commission to overturn its previously ruling that utilities only provide customer data to law enforcement with proper legal service.[16]

As Smart Grid technologies continue to collect ever more finely-grained data about household habits, law enforcement officials will become even more interested in accessing that data to develop cases. In investigating crimes, for example, agencies may want to establish or confirm presence at an address at a certain critical time; this information may be gleaned from smart meter reading data or temperature inside the home collected by a programmable thermostat.

---

[11] For more about recent trends in data aggregation and the development of enhanced customer profiles for advertising purposes, see CDT, *CDT's Guide to Behavioral Advertising*, http://cdt.org/privacy/targeting/.
[12] 533 U.S. 27 (2001).
[13] *Id.* at 30.
[14] *United States v. Kyllo*, 809 F. Supp. 787, 790 (D. Or. 1992), *aff'd*, 190 F.3d 1041 (9th Cir. 1999), *rev'd*, 533 U.S. 27 (2001).
[15] Jo Moreland, *Drug Raid Has Carlsbad Family Seeing Red*, N. County Times, Mar. 25, 2004, *available at* http://www.nctimes.com/news/local/article_ea2047e8-59e1-551e-b173-ce89ffad4d90.html.
[16] D.01-07-032 at 1.

While Smart Grid data certainly may be useful for these purposes, the privacy implications of law enforcement access, especially in the traditionally protected area of the home, call for strong, constitutionally adequate protections for this information, careful procedures on the part of utilities and others with access to this data, and technology design that allows for strong data protection.

3. Civil Litigants' Incentives to Acquire Customer Energy Data Create Privacy Risks

Civil litigants may also place a high value on detailed energy usage data. For instance, an insurance company contesting a homeowner's claim might seek access to the homeowner's energy data to disprove that he actually owned the specific appliances he claimed. Similarly, in a custody proceeding, a spouse may seek energy data to show the other spouse took the children out of the state for two days without proper consent. In both cases, the detailed usage data would certainly be relevant to proving or disproving the contested fact. As with access by government agencies, effective procedural protections should be required, as should careful procedures for managing civil requests on the part of utilities and other providers. These include first requiring litigants to seek data from the customer directly (who, under our recommendations, should have access to data pertaining to his or her home energy usage). If the only way to obtain the information is directly from a regulable entity, then the litigant should be required to show a compelling interest in the information, and the entity should provide energy customers with notice and an opportunity to object before disclosing data.

4. Criminal Incentives to Acquire Customer Energy Data Create Privacy Risks

Criminals might also seek access to smart meter data or other information collected by the Smart Grid, in hopes of using this data to infer whether anybody is present in a house and to determine the most desirable time to commit a crime. In addition, because the Smart Grid enables the accumulation of personally identifiable and other revealing information over long periods of time, information-gathering via Smart Grid technologies could reveal behavior patterns likely to be repeated in the future, allowing criminals to plan for future crimes. The information could also be used by criminals to commit identity theft, especially if utilities or other providers use unsecured paths to transmit data. For instance, many utilities use energy

consumption data to authenticate customers, making the information particularly valuable to those attempting illicitly to take over someone else's account.[17] Failing to encrypt data transmission within the Smart Grid compounds these threats to customer data security.

C. Current Privacy Legal Frameworks Offer Some Protections for Energy Data But Are Insufficient to Fully Protect Data in the Smart Grid

The significant privacy risks to consumers, described above, are compounded by the dearth of clear rules that apply to the new technology landscape. As the National Institute of Standards and Technology (NIST) noted in its First Draft NISTIR 7628, there remains a "lack of consistent and comprehensive privacy policies, standards, and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use," creating "a privacy risk that needs to be addressed."[18]

In this proceeding, the Commission has been presented with the important opportunity and responsibility[19] to develop privacy protections for California citizens' energy data. Both the California and Federal Constitutions, as well as various regulatory decisions and provisions, provide some protections for energy data, but these protections were not designed to cover the unprecedented volume of data, nor varieties of new data, that the Smart Grid will make available about household activities. As such, these protections need to be supplemented to ensure that Californians can continue to enjoy the level of privacy they expect and are entitled to in their homes.

Historically, the principal source of privacy regulation for electricity data has been state public utility commissions, which place varying restrictions on disclosure of consumer energy data.[20] Generally, state utility commissions are just beginning to consider the privacy implications of Smart Grid data, putting California in a leadership position.[21] Because the

---

[17] For instance, San Diego Gas and Electric (SDGE) uses the amount of the last SDGE bill to authenticate its customers when the customers sign up for an online account. *See* SDGE, *My Account*, https://myaccount.sdge.com/myAccountUserManager/pageflows/usermanager/Registration/begin.do.

[18] Nat'l Inst. of Standards & Tech., *Draft NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements* (2009), *available at* http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf.

[19] *See, e.g.*, D.09-12-046 at 26 (finding that the Commission should create rules about privacy and security to protect customers); D.90-12-121 at 11 (holding that utilities can only provide data to law enforcement pursuant to legal process).

[20] Quinn, *supra* note 6, at 24.

[21] For example, the National Association of Regulatory Utility Commissioners (NARUC) will consider a resolution in 2010 that would encourage member states to support several regulatory protections on consumer data collected in

existing laws alone do not provide adequate protection for the categories and quantities of data that the Smart Grid will generate, the Commission should use its regulatory authority to ensure that the Smart Grid does not undermine the privacy protections guaranteed to California citizens.

Specifically, as we describe in later sections, the Commission should (1) define the scope of customer energy data that warrants privacy protection, (2) broadly adopt cyber security and privacy principles to ensure that smart grid proposals will provide sufficient privacy protections, (3) require utilities to employ Fair Information Practice principles (FIPs) as part of Smart Grid deployment plans, (4) provide additional privacy protections in the Proposed Access Rule, (5) request privacy-related quantitative metrics from utilities in smart grid implementations, and finally, (6) the Commission should not wait for privacy standards from the national standard-setting bodies, but should adopt FIPs immediately.

III. The Commission's Authority to Regulate Consumer Privacy and Data Access Issues on the Smart Grid Is Derived from the California Constitution, Senate Bill 17 and the Commission's Past Decisions

The Commission stated its policy objective in D.09-12-046 to "[e]nsure all information is secure and that a customer's privacy is protected."[22] It further stated it would require utilities put in place "sufficient privacy and security measures . . . to mitigate the potential for fraud and hacking" and that "access to usage data must be provided consistent with the rules [the Commission] adopt[s] to ensure that access is provided consistent with EISA, the general public interest, and state privacy rules."[23]

The California Constitution's privacy provision,[24] along with Senate Bill 17,[25] support these goals and provide the Commission with broad authority to adopt rules and protocols designed to protect and preserve consumer privacy rights. We discuss these and additional grounds for the Commission's authority in this section.

---

the Smart Grid. *See* NARUC, *Draft Resolutions Proposed for Consideration at the 2009 Annual Convention of NARUC* 14-17 (2009), *available at* http://annual.narucmeetings.org/09_1106_Proposed_Resolutions.pdf; *see also* Nat'l Inst. of Standards & Tech., *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0*, at 84 (2009), *available at* http://www.nist.gov/public_affairs/releases/smartgrid_interoperability.pdf.

[22] D.09-12-046.

[23] *Id.*

[24] Cal. Const. art. 1, § 1.

[25] Specifically Cal. Pub. Util. Code §§ 8360(i), (j).

In *White v. Davis*[26] the California Supreme Court explained that "the moving force" behind California's constitutional right to privacy "was a more focused privacy concern, relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society," and that its "primary purpose is to afford individuals some measure of protection against this most modern threat to personal privacy."[27]

Importantly, our state constitutional privacy right protects Californians against private businesses as well as the government. As the *White* court put it, the right "prevents government and business interests from collecting and stockpiling unnecessary information about us," partly because "[t]he proliferation of government and business records over which we have no control limits our ability to control our personal lives."[28] Thus, among the "principal 'mischiefs'" targeted by the constitutional right are "the overbroad collection and retention of unnecessary personal information by government and business interests" and "the improper use of information properly obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party."[29]

The Commission has recognized its constitutional obligations to protect privacy in past decisions. When confronted with the consumer privacy concerns presented by telephone monitoring technologies, in Decision No. 88232, the Commission unequivocally stated that, "[o]ur constitutional responsibilities and those of the utilities we regulate, are paramount. . . ."[30] In *The Matter of the Application of Pacific Bell,* when confronted with the consumer privacy concerns presented by Pacific Bell's default installation of caller identification technology, the Commission drew upon its constitutionally granted authorities and rightly refused to allow commercial expediency to take precedent over the rights of California citizens. It stated:

> If the service is to be offered consistently with constitutional guarantees and the public interest, it must be offered in a way that maximizes the ease and freedom with which California citizens may choose not to disclose their calling party numbers. We will not compromise an individual's free exercise of his or her right of privacy in order to place in the hands of the Caller ID subscriber a more valuable mailing list, a marginally better

---

[26] *White v. Davis*, 13 Cal.3d 757 (1975).
[27] *Id.* at 774.
[28] *Id.*
[29] *Id.* at 775.
[30] *In re PT&T Co.*, 83 C.P.U.C. 149 (1977).

> method of screening or managing telephone calls, or even a slightly more effective deterrent to unlawful or abusive uses of the telephone.[31]

Smart Grid technology poses far greater, yet far less visible, threats to consumer privacy than Caller ID. Unlike Caller ID, which only transmits the caller's phone number, Smart Grid technologies can reveal minute details about the lives in a household. This suggests even greater reason for the Commission to address these issues. Further, these precedents strongly support interpreting the Commission's constitutional obligations to include protecting consumers from the full range of privacy threats.

California State Senate Bill 17 (Padilla), which added sections 8360 through 8369 to the California Public Utility Code, also provides the requisite authority to protect consumer privacy. Specifically, section 8360(i) requires that the Commission "[d]evelop standards for communication and interoperability of appliances and equipment connected to the electric grid."[32] The Commission is empowered to regulate the privacy and security of consumer energy data because such privacy and security are critical aspects of any "standards for communication." Likewise in section 8360(j), the legislature has tasked the Commission with "[i]dentifying and lowering [ ] unreasonable or unnecessary barriers to adoption of smart grid technologies, practices, and services." Because customers will be dissuaded from adopting Smart Grid technologies unless the risk to privacy posed by such technologies is addressed, the Commission can and should use its authority under section 8360 to create consumer privacy protections, thus lowering resistance to adoption.

IV. The Commission Should Define the Scope of Customer Data that Warrants Privacy Protection

Designing an effective framework to protect customer data requires a specific articulation of what information requires protection. We recommend that the Commission adopt a robust and expanded interpretation of the term "customer information" to account for the new types of information on the Smart Grid. The Commission should then act to regulate the collection, use, and dissemination of that customer information as we describe in subsequent sections.

---

[31] *In re Pacific Bell*, 44 C.P.U.C.2d 694 (1992).
[32] Cal. Pub. Util. Code § 8360(i).

The California Public Utility Code currently describes "customer information" in section 394.4 as including "customer specific billing, credit, or usage information."[33] This section importantly requires Electric Service Providers to treat such information as confidential unless the customer consents otherwise in writing.[34] Affiliate Transaction Rule IV.A similarly articulates the confidentiality requirement that attaches to customer information, in this case, when the information is in the hands of the utilities.[35] The rule provides that: a "utility shall provide customer information to its affiliates and unaffiliated entities on a strictly non-discriminatory basis, and *only with prior affirmative customer written consent.*[36]

"Customer information" should be construed to cover the broad set of intimate information that is now collectable within the Smart Grid and should apply to all entities collecting, storing or transmitting customer data. We suggest that, beyond its current denotation, the term be expressly interpreted to include all usage data and device data capable of revealing either personally identifiable information or household-identifiable information.[37] Specifically, the Commission should expressly interpret the meaning of "customer information" to include:

> (1) *traditional personally identifiable information* (PII), such as account information used for billing purposes and unique device identifiers tied to an individual name, which is either immediately personally identifiable or becomes personally identifiable when combined with other collected information;
>
> (2) *data collected about an individual household* in the Smart Grid that is revealing of home life by itself or when analyzed or combined with other information. Examples of this second category of data include, without limitation: granular usage data from individual households, records of plug-in hybrid electric vehicle (PHEV) use, and specific metering and device data (e.g. thermostat temperature); and

---

[33] *See* Cal. Pub. Util. Code § 394.4(a) ("Customer information shall be confidential unless the customer consents in writing. This shall encompass confidentiality of customer specific billing, credit, or usage information.").
[34] *See id.*
[35] D.97-12-088, app. A, Rule IV.A, *rev'd by* D.98-08-035, *amended by* D.98-12-075.
[36] *Id.* (emphasis added).
[37] This distinction between personal identifiability and household identifiability is intended to emphasize the importance of protecting the privacy of households, in addition to the privacy of individual persons. We focus here on protections that the home and household deserve, but we note that the energy usage data of organizations such as churches, political associations, and medical offices may warrant similarly strong protections.

(3) *energy usage data collected from the home by entities without the permission or intervention of the utility*, to the extent that the authority of the Commission covers such entities.

Sometimes information in the second category will be personally identifiable when combined with other types of information or when the number of people in a household is small. Regardless of whether it is individually identifiable, however, household-identifiable information is inherently revealing of household activities and home life, traditionally private domains that are, and should continue to be, protected from observation. It can still reveal highly personal and invasive details about daily activities of people living in the home, such as the use of a specific medical device or an absence from the home, raising serious privacy issues. Further, given that 32.2 million people live alone in the U.S. and twenty eight percent of American households have single-person occupancy,[38] household-identifiable information is functionally equivalent to "personally identifiable information" for a significant number of consumers.

The principles discussed here for customer information outline the minimum protections required for this basic category of data. Some of the information included within the customer information, such as PII and location-identifying information, will require additional protections.

V. The Commission Should Adopt Privacy and Security Principles Based on the Fair Information Practice Principles (FIPs) to Ensure that Smart Grid Proposals Will Provide the Privacy Protections Required by State and Federal Law

In section 5.5 of the Joint Ruling, the Commission asks broadly what cyber security and privacy principles Smart Grid proposals should meet.[39] As has also been discussed at length elsewhere,[40] the privacy issues associated with home energy usage data can and should be addressed through robust application of the full set of FIPs. We strongly urge the Commission to use the FIPs as a general overarching framework to guide the privacy principles and rules it adopts. These principles reflect international guidelines, and go beyond the currently dominant—

---

[38] U.S. Census Bureau, *Facts for Features: Unmarried and Single Americans Week*, July 21, 2009, http://www.census.gov/Press-Release/www/releases/archives/facts_for_features_special_editions/014004.html.

[39] *Assigned Commissioner and Administrative Law Judge's Joint Ruling Amending Scoping Memo and Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid* 33-39 (Feb. 8, 2010) [hereinafter "Feb. Joint Ruling"].

[40] *See* CDT, *Comments of the Center for Democracy & Technology on Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security and Requirements, National Institute of Standards and Technology* (2009) *available at* http://www.cdt.org/files/pdfs/CDT%20Comment%20NISTIR%207628%20Draft%2012-02-09%20FINAL%20-%20updated.pdf.

and discredited[41]—model of "notice and choice." The FIPs have been used for information management since 1973 and provide a well-tested framework for balancing and harmonizing privacy concerns with other interests. They have gained broad acceptance by national and international privacy regulators and have been applied in many contexts related to consumer privacy. The FIPs are well-aligned with the requirements of SB 17. Properly formulated and rigorously implemented, the FIPs provide a broad, comprehensive privacy framework that should underlie all privacy principles for Smart Grid deployment. Adopting FIPs as a framework is an essential part of protecting consumer privacy and ensuring that the Smart Grid maximizes "benefit to ratepayers"[42] by creating a system that carefully weighs the tradeoffs between disclosure and privacy protection.

A. The Fair Information Practice Principles

The Commission should adopt the FIPs framework because it provides a complete system for considering privacy and consumer security issues. We rely here on the articulation of the FIPs recently adopted by the US Department of Homeland Security,[43] on the belief that a framework developed for information systems affecting the national security is also well-suited to the issues posed by the Smart Grid. The DHS framework includes the following eight principles: (1) Transparency, (2) Individual Participation, (3) Purpose Specification, (4) Data Minimization, (5) Use Limitation, (6) Data Quality and Integrity, (7) Security, and (8) Accountability and Auditing. These principles are described at length in this section and referred to extensively throughout our recommendations in the sections that follow.

1. **Transparency:** Data management practices should be transparent and should provide meaningful, clear, full notice to the consumer regarding the collection, use, dissemination, and maintenance of customer information.

An entity that handles customer information must make comprehensive and accurate disclosures to customers about the collection, use, dissemination and maintenance of customer

---

[41] For example, National Telecommunications and Information Administration Associate Director for Domestic Policy Daniel J. Weitzner recently stated "[t]here are essentially no defenders anymore of the pure notice-and-choice model." *See* Steve Lohr, *Redrawing the Route to Online Privacy*, N.Y. Times, Feb. 28, 2010, *at* Bus. 4, http://www.nytimes.com/2010/02/28/technology/internet/28unbox.html (quoting Mr. Weitzner).

[42] SB 17.

[43] *See*, U.S. Dept. of Homeland Sec., *Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

information. This disclosure must be made to the consumer prior to any collection. This information-sharing must extend beyond mere notice of collection practices; it must also include providing consumers with clear, detailed information about the specific uses of their data, retention periods, and any transfers of data to or access by other entities. Notices should state clearly: what information is collected, whether this information is shared and with whom it is shared, the period that data is retained, and the contact information for an official at each company responsible for the policy and for personal data collected by the system. Further, Smart Grid entities, including utilities, should also provide consumers with access to the personally identifying information collected about them, as well as all usage data collected about their homes. This principle aligns closely with section 8360(h), which requires that consumers be provided with "timely information and control options."[44] This principle is also essential to the successful implementation of many of the following principles, especially Individual Participation and Accountability and Auditing.

2. **Individual Participation:** Regulable entities should involve the individual in the process when they use customer information and, to the extent practicable, seek ratepayer consent for the collection, use, dissemination, and maintenance of customer information.

New smart meters create the need for regulable entities to give customers a choice about the types of customer information collected and its use, transfer, and maintenance, including retention. To fully recognize the principle of individual participation, regulable entities must respect the range of consumer preferences with respect to their data that will exist at multiple points along the data path.

Under the Public Utilities Code, customer information, including usage information, is confidential.[45] To protect consumer privacy, regulable entities should be required to get affirmative written customer consent prior to the collection and use of customer information for any secondary purposes beyond what is strictly required for the provision of service. Consumers implicitly agree to the minimum data disclosures required for utilities to provide energy generation and billing. However, any other uses that are not strictly necessary require affirmative consent. For example, affirmative written consent would be required for a utility to

[44] Cal. Pub. Util. Code § 8360(h).
[45] *Id.* § 394.4(a).

use customer information for delivering advertisements to its customers because it is not strictly necessary to the primary purpose of providing energy service.

3. **Purpose Specification:** Regulable entities should specifically articulate the purpose or purposes for which customer information will be used.

Regulable entities should provide consumers with information about how the entity will use their data *before* the time of collection. The specification of purpose should fully describe the purposes for which the data being collected will be used. These will likely include uses of customer energy data necessary for core entity operations and services, such as efficient and reliable delivery of electricity, demand response, and billing. To the extent that utilities plan to use data for purposes not strictly necessary to the performance of core operations and services, such as marketing, customers should also have sufficient opportunity to separately and expressly consent to such uses.

Clearly articulating the purpose of data use enables the consumer to make an informed choice before deciding to share data. In the context of the Smart Grid, for example, one would expect a utility to specify to a consumer that "customer information" will be used for the purposes of providing time-of-use pricing that may reflect discounted rates during certain times of the day. If a utility plans to share customer information with any third-party service providers, the utility must disclose that fact along with all uses for which the third-party will use the data. If the utility later wishes to change the purpose for which the customer information is used, the utility must first notify consumers and give them the choice whether to consent to that new use.

4. **Data Minimization:** Only data directly relevant and necessary to accomplish a specified purpose should be collected, and data should only be retained for as long as necessary to fulfill the specified purpose.

Generally, Smart Grid standards should support, and technologies should be capable of, appropriate data minimization. The Data Minimization principle dictates that regulable entities may only collect and maintain customer data necessary for the performance of specified purposes, as defined above.[46] Unnecessary information should not be collected; as soon as collected information becomes unnecessary for a stated purpose, it should be deleted.[47]

---

[46] *See supra* § V.A.3.

[47] OpenADR is an example of a technology that can contribute to data minimization by significantly reducing data collection while still enabling demand response functionality. Demand Response Research Ctr., CEC-500-2009-

In addition to supporting consumers' privacy interests, data minimization is an important part of Smart Grid cyber security, which the Commission is responsible for overseeing under section 8360(b) of SB 17, and also is important to protecting customer safety as required by section 8363.[48] As previously discussed, energy data could be used for many unauthorized and sometimes malicious purposes.[49] Minimizing data collection is a powerful tool for protecting against these security and privacy threats: if the data does not exist, it cannot be compromised. Therefore, adequate minimization requirements for the data that regulable entities collect and keep will address security and privacy concerns, while leaving untouched the data that entities need to fulfill their core operations.

The initial technical architecture that regulable entities adopt to implement the Smart Grid can have a substantial impact on the long-term scope of their data collection practices. For example, collecting and aggregating usage data at the meter level (or household level) could help protect consumer privacy through data minimization. Smart meters deployed in California are already furnished with memory and processing power. The current smart meters could compute electricity bills based on time-of-use pricing, and only periodically transmit aggregate usage and billing information back to the utility, at user defined time spans such as weekly or monthly. These changes would not affect the accuracy of billing or reveal the consumer's consumption data on a granular level to the utility. Yet, all smart meters are not equally smart. When a utility installs smart meters that do not have aggregation capabilities, consumers lose their ability to choose what level of data the utility can see. Consequently, they may surrender more data than the utility actually needs.

Consumers should be provided with tools to aggregate their energy usage data at the meter level before the data is sent along. Consumers should be able to decide the frequency of aggregated smart meter data reported to regulable entities. This requirement is easily implemented because smart meters can be remotely updated, which is all that is required to implement this aggregation function. Provide consumers with tools to decide the time intervals

---

063, *CEC OpenADR-Version 1.0 Report* 1 (Pier Final Project Report, 2009) *available at* http://openadr.lbl.gov/pdf/cec-500-2009-063.pdf (last visited Mar. 9, 2010).

[48] Cal. Pub. Util. Code §§ 8360, 8363.

[49] *See supra* § II.B.

of smart meter reading reported enables households to fully participate in the decision to share their customer information outside of the home.[50]

Residential energy management systems also can minimize data collection by regulable entities. Instead of registering individual smart devices with utilities, consumers could use residential energy management systems, under their control, to manage their devices.[51] In this architecture, smart devices only register with consumers' own residential energy management systems and are invisible to the utilities and other regulable entities who communicate directly with the residential energy management system.[52] Residential energy management systems are being actively developed by commercial entities[53] as well as researchers at University of California.[54]

Importantly, it is presently unclear whether utilities need to collect information about the functioning of individual appliances, or even individual houses, in order to implement effective load management or demand response programs. For many purposes and programs, such detailed data should not be necessary. Given the privacy interests in household-level usage data, the collection and use of it should be subject to scrutiny. Because entities seeking to collect this type of data are in the best position to demonstrate why it is needed, these entities should bear the burden of proving the need for granular customer information, and should be required to show why it is necessary for specific purposes.

The Commission should also apply the Data Minimization principle to regulable entities' data retention practices and should consider revising the current retention periods for customer records, which widely reflect the industry standard of seven years.[55] Although regulable entities may need to retain some data like billing records and load research data for longer periods of time, they should be required to destroy unrelated or unnecessary data. For example, for billing

---

[50] Minimizing the data that leaves the home is especially important because of the well-established constitutional protections for data residing in the home, as discussed, *supra*, § II.C.

[51] S. Cal. Edison, *SmartConnect Use Case: C6 - Customer Uses an Energy Management System (EMS) or In-Home Display (IHD)*, at 18 (2009), *available at* http://www.sce.com/NR/rdonlyres/C39473B2-50BF-48C6-BAC7-4904DEE0D51F/0/C6_Use_Case_090105.pdf.

[52] *Id.*

[53] Press Release, Tendril, Tendril Achieves First Open ADR Compliant Platform (Jan. 29, 2009) *available at* http://www.tendrilinc.com/2009/01/tendril-achieves-first-open-adr-compliant-platform-2/.

[54] David Auslander & Daniel Arnold, Reference Design for Residential Energy Gateway, http://mechatronics.berkeley.edu/gateway.htm (last visited Mar. 9, 2009).

[55] *See* P.S. Subrahamanyam, David Wagner, Deirdre Mulligan, Erin Jones, Umesh Shankar, & Jack Lerner, CyberKnowledge & Univ. of Cal. at Berkeley, *Network Security Architecture for Demand Response/Sensor Networks* 87 (2006), *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/demand_response_CEC.pdf.

purposes the utility may need monthly totals of energy consumption; however it would not need to keep the intermediate granular measurements of consumption and load. Beyond the security advantages of reducing retention, shorter periods will likely yield benefits to regulable entities in terms of decreased storage and maintenance costs.[56] Monthly totals are less revealing and serve an important record-keeping purpose and can thus justifiably be retained for longer than near-real-time consumption information.

5. **Use Limitation:** Customer information should be used solely for the purposes specified in the notice. Sharing of such information should be only for a purpose compatible with the purpose for which it was collected.

Where regulable entities collect customer information for the primary purpose of providing energy service to the ratepayer, access to that data should be limited within the entity to departments with a justifiable requirement to use the data for fulfilling the clearly-specified purpose, such as the billing department. Any secondary uses beyond those must be specified in advance, and should only occur with explicit consumer consent under an affirmative consent regime, as introduced above.[57] For example, detailed information about a consumer's smart devices, such as a MAC address uniquely identifying the device and the manufacturer of the device, should not be used by a regulable entity or third party service provider, unless such use was specified to the consumer, who specifically and affirmatively consented to the use. Similarly, the entity should not share customer information or use it for behavioral advertising or other marketing purposes on behalf of a third party without explicit written authorization from the consumer. The Commission should require regulable entities to explain how they implement these use limitations.

6. **Data Quality and Integrity:** Regulable entities should, to the extent practicable, ensure that data is accurate, relevant, timely and complete. Regulable entities should provide consumers with tools to correct mistakes or challenge information provided in profiles.

Consumers need to be able to review and, where necessary, correct their information. This is required by section 8360(h), which states that customers must be provided information

---

[56] Robert Gellman, *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete* (2002), http://epic.org/reports/dmfprivacy.html.
[57] *See supra* § V.A.2

and control options.[58] To comply with this requirement, the Commission should require regulable entities implement standards and technical requirements that will allow for easily-accessible interfaces that give consumers the opportunity to review and correct their customer information. Such review provides the best means of ensuring that consumer data is accurate.

7. **Data Security:** Regulable entities must protect customer information through appropriate security safeguards against risks of loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure, and Smart Grid technologies and services must be capable of implementing these security safeguards.

Reasonable security in the Smart Grid requires that any transmission of customer information must be secure and that regulable entities' data practices include meaningful safeguards for customer information. For example, encryption should be required for all communications that are sent over open wireless protocols or that could otherwise reasonably be intercepted on organization-owned infrastructure and third-party communication services. More broadly, the Commission should review technical standards for implementation and, if necessary, revise them to require that smart device communications provided by regulable entities be truly secure.

Further, customer information collected, used and maintained by regulable entities must be stored securely, made available only to those with a documented and authorized need for the information, and must be maintained subject to secure data management practices. If a security or other breach results in the loss or exposure of customer information, the regulable entity should be required to notify affected customers and take all reasonable steps to minimize harm to customers.

8. **Accountability and Auditing:** Regulable entities should be accountable for complying with these principles, should provide appropriate training to all employees and contractors who use customer information and should audit the actual use of that information to demonstrate compliance with the principles and all applicable privacy protection requirements.

The Commission should require regulable entities to have regular privacy training and ongoing awareness activities. Systems storing customer information should have access logs to document who is accessing private data. The Commission should require regulable entities to

[58] *See* Cal. Pub. Util. Code § 8360(h).

conduct regular audits of these logs to ensure that access is in compliance with appropriate and disclosed uses of the data. The Commission should further require rigorous reporting and auditing requirements that examine regulable entities' compliance and adoption of each of these privacy principles. Without a robust accountability and auditing mechanism, there will be no way for the Commission to ensure compliance with the various privacy commitments utilities make in their Smart Grid deployment plans.

B. The Principle of "Data Ownership" Alone Will Not Create Sufficient Privacy Protections for Consumers and Must Be Supplemented with the Fair Information Practice Principles

Consumer data ownership rules are often discussed as potential solution to privacy concerns. Although we generally support consumer ownership of data (assigning data ownership to utilities would turn them into information gatekeepers and could impede realization of both privacy and innovation policy goals), consumer ownership, alone, rarely solves privacy and security issues. Data ownership without attendant and real control over data can leave consumers with the limited ability to choose between alienating their data or not. Utilities and other third parties may require consumers to surrender control, if not ownership of customer information as part of service agreements and conditions of service. Instead, consumers need ongoing rights in their data—regardless of where it is stored and by whom it is held—complimented by assurances that those to whom they entrust it are bound by clear rules requiring them to abide by consumers' decisions. Such a framework respects the ongoing implications such data has for the consumer's privacy and safety.

The FIPs provide this broader privacy framework. FIPs do not require a specific data ownership regime, but are compatible with and complimentary to consumer data ownership. In particular the Transparency and Purpose Specification principles, discussed above in this section, ensure the data owner can make informed decisions about authorizing uses of data. The requirements of Data Quality and Integrity help the consumer maintain control over his data even when it is held by another party.

We encourage the Commission to recognize a consumer's ownership interest in customer information. However, to provide meaningful protections, the Commission needs to issue regulations that give consumers real control over their data even when it is held by third parties. The Fair Information Practice principles should provide the framework for the protections

necessary to ensure that utilities cannot force or induce consumers to contract away all their rights in their data, depriving them of any privacy protections.

C. Security and Privacy Principles Adopted by the Commission Should Specifically Require Data Breach Notification

Data breach notification is an important privacy practice implicated by the FIPs Data Security Principle. It warrants further elaboration and special attention by the Commission. California's Data Breach Notification Law, section 1789.29 of the Civil Code, made California a leader in data breach notification by requiring entities to report any breach in security to a system that contains personally identifiable information to all impacted individuals.[59] Forty-four other states have followed California's lead in this matter.[60]

We urge the Commission to keep California in the forefront of data breach notification by applying the requirements of section 1789.29 to regulable entities as part of their Smart Grid proposals. They should be required to report any breach of security in customer information to all impacted consumers and to the Commission.

Data breach notification rules will provide additional incentives for regulable entities to develop strong privacy and security standards. The cost and embarrassment resulting from breach notification can be a strong motivator. Further, by providing consumers' notice of data breaches, they can take appropriate measures to protect themselves from identity theft and other possible crimes. These notifications can also help the public and the Commission to evaluate regulable entities' security efforts.

VI. To Fulfill the Requirements of Senate Bill 17, the Commission Should Require Utilities to Employ Fair Information Practice Principles as Part of Utility Smart Grid Deployment Plans

The Commission has been tasked with determining the requirements for a Smart Grid deployment plan, which will guide the utilities in the development of their individual deployment plans.[61] It has asked for comments on the topics that should be addressed by the utilities'

---

[59] Cal. Civ. Code §§ 1798.29, 1798.82.

[60] Perkins Coie, *Security Breach Notification Chart* 134-35 (2008), *available at* http://www.digestiblelaw.com/files/upload/securitybreach.pdf (listing the effective dates for all forty-five states, plus Puerto Rico, that have enacted data breach notification laws).

[61] Feb. Joint Ruling, *supra* note 39, at 3.

plans.[62] It has also sought comment upon the proper evaluation and use of those deployment plans by the Commission.[63] We address both of these questions here.

In section V above, we have urged the Commission to adopt FIPs as a framework for ensuring privacy protections on the Smart Grid. Here, we specifically urge the Commission to incorporate the FIPs as requirements within the Smart Grid deployment plans. Specifically, utilities' deployment plans should take into account each of the following: (1) Transparency; (2) Individual Participation; (3) Purpose Specification; (4) Data Minimization; (5) Use Limitation; (6) Data Quality and Integrity; (7) Security; and (8) Accountability and Auditing.[64]

The Commission should ensure the privacy of the Smart Grid by requiring utilities to use the FIPs as part of their deployment plans in the following four ways. First, based on the FIPs, the Commission should define baseline privacy standards for Smart Grid deployment. Second, the Commission should require each utility to perform a privacy impact assessment as part of its Smart Grid planning process. Third, based on the assessment, each utility should adopt privacy practices meeting the minimum standards set by the Commission. These privacy practices should be responsive to each of the FIPs principles. Finally, the privacy impact assessments and the resulting privacy policies within the utilities' deployment plans should be revisited and re-approved in subsequent ratemakings and each time the Commission approves further investment pertaining to Smart Grid and Smart Device deployment. Only by an iterative process of problem definition, analysis, adoption, and review can the Commission and Californians be assured that their private information is being protected.

As part of the privacy impact assessment required by FIPs, a utility—in advance of actually building and deploying a system—would be required to answer key questions posed by the FIPs: What data will the utility be collecting? For what purpose? With whom will it share the data? How long will it keep the data? What confidence does it have that the data will be accurate and reliable enough for the purposes for which it will be used? How will it protect the data against loss or misuse? How will individuals have access to data about themselves? What audit, oversight and enforcement mechanisms will it have in place to ensure that it is following its own rules? The answers to these questions will provide important insights in the privacy and

---

[62] *Id.*
[63] *Id.* at 5-8.
[64] For a detailed discussion of these principles, please see *supra* § V.

security issues created by the Smart Grid. By identifying them early utilities can mitigate and guard against risks and protect consumer privacy at the lowest possible cost.

A. The Commission Should Require Regular Review of Privacy Impact Assessments and the Resulting Privacy Policies Contained in Deployment Plans

To ensure compliance with the deployment plan requirements described above, the Commission should require periodic reviews of privacy impact assessments and privacy policies. Utilities should be required to evaluate their implementation and success of their privacy policies and report their findings to the Commission. Further, the Commission should require appropriate revisions to the privacy impact assessments and privacy policies when deployment plans are modified. Similarly, new assessments and policies should be completed prior to any new deployment or revision to Smart Grid architecture. Any privacy lapses or data breaches should be evaluated by the Commission prior to awarding new rates or approving new deployments to determine if the utility is taking and has taken appropriate steps to remedy the problem and generally to protect privacy.

B. Privacy Considerations Must Be Built into the Design of the Smart Grid

Deployment plans can provide utilities an opportunity to address privacy concerns at an early design stage. Requiring strong privacy protections from the design stage will enable California's Smart Grid to maximize privacy and utility, while minimizing the cost of the protections. The Commission should require utilities adopt a "privacy by design" approach,[65] and build standards that reflect privacy interests into their deployment plans, rather than attempting to tack on privacy at a later point. Privacy by design is an effective and economically efficient means of protecting consumer privacy and security. Embedding privacy protections into the technology and design now, before smart meters and other Smart Grid technologies are fully deployed, and before the telecommunications infrastructures are installed, will prove less expensive than attempting to address these issues in the future and will make the grid more adaptable to changing threats to privacy and security as use increases.

---

[65] *See* Ann Cavoukian, Info. & Privacy Comm'r of Ont., *Privacy by Design*, http://www.privacybydesign.ca/ (last visited Mar. 9, 2010).

VII. The Commission Should Consider and Adopt Our Recommended Modification to the Proposed Access Rule, as Provided in Appendix A

As the February 8, 2010 Joint Ruling notes, "[t]he Commission has adopted a policy to provide that some third parties can have access to [customer] data with the customer's permission."[66] The ruling goes on to express concern about a number of unintended and unauthorized uses of the data that the Smart Grid may effectuate. Third-party access to customer data may support third-party services that provide some of the benefits of the Smart Grid; at the same time, third-party access represents its greatest privacy threat. A utility, for example, is specifically subject to this Commission's rules and specific statutes that limit data use and disclosure.[67] A non-utility third party possessing the same data, on the other hand, may not face the same obligations, though general prohibitions against unfair or deceptive data practices (e.g., FTC Act § 5) and state security breach notification laws would apply. We support the Commission's suggestion to require customer authorization before a utility provides customer data to any third party. However, given the highly personal nature of the data that would potentially be shared, the Commission should adopt a strong privacy standard in its Proposed Access Rule[68] and should condition access on requirements that follow the Fair Information Practice principles.

Some third parties seeking access to customer data are likely to have business models based upon offering the consumer a service, perhaps for free, and then commercializing and selling the data. For example, a third-party service given access to granular usage data could offer consumers a useful service that helps them understand and control their energy consumption but base its profits on analyzing and selling behavioral information of interest to advertisers. Electronics retailers would like to know what appliances are in the home so they

---

[66] Feb. Joint Ruling, *supra* note 39, at 34.

[67] *See, e.g.*, Cal. Pub. Util. Code § 394.4 (requiring electric service providers to keep "customer information"—which encompasses "customer specific billing, credit, or usage information"—confidential unless the customer gives written consent to disclosure); D.97-12-088, app. A, § IV.A, *available at* ftp://ftp.cpuc.ca.gov/gopher-data/energy_division/affiliate/R9704011-Appendix%20A.doc ("A utility shall provide customer information to its affiliates and unaffiliated entities on a strictly non-discriminatory basis, and only with prior affirmative customer written consent."); Pac. Gas & Elec., *Rule 22 - Direct Access Rules* § C.3.a (1997), *available at* http://www.pge.com/tariffs/tm2/pdf/ELEC_RULES_22.pdf (requiring a customer to give written authorization for a utility to disclose usage data to direct access service providers); S.D. Gas & Elec., *Rule 25 - Direct Access Rules* § C.3.a (1999), *available at* http://www.sdge.com/tm2/pdf/ELEC_ELEC-RULES_ERULE25.pdf (same); S. Cal. Edison, *Rule 22 - Direct Access Rules* § C.3.a (2001), *available at* http://www.sce.com/NR/sc3/tm2/pdf/Rule22.pdf (same).

[68] Feb. Joint Ruling, *supra* note 39, app. B.

can market upgrades and accessories. A health insurance company may be interested in the number of hours a customer spends in front of the television. A dating website might be interested knowing that the number of residents at the household had recently fallen from two to one.

The consequences of utilities transferring customer data to third parties are significant. First, every copy and transmission of the data increases the risk of security breaches. Second, third parties may use the data in inappropriate or undisclosed ways. Third, the third parties may transfer the data on to yet other parties. Without proper protections, the customer could lose all control of her data once she authorizes third-party access. Customer trust in the Smart Grid is essential to its successful deployment and full adoption. Third-party misuse of data could be enough to undermine that trust. Therefore, the Commission's third-party data access rule should require utilities that deal with third parties to take appropriate steps to ensure that the third parties receiving data will provide appropriate privacy and confidentiality protections.

To actively protect against unexpected uses and the resulting harms, the Commission should adopt a robust regulatory framework granting affirmative control to customers as it extends to data generated by their households. This regulatory framework should attempt to maximize customer control over data and privacy protection, while enabling the benefits of the Smart Grid.

To reconcile these twin objectives, we propose a number of general changes to the Proposed Access Rule, based upon the Fair Information Practice principles. First, utilities should be required to obtain customer authorization based upon the full and complete disclosure of the uses that third parties will make of the data prior to giving third parties access to that information. If consumers agree to allow third-party access to such intimate information, the customer should be on specific notice of all uses prior to giving authorization. Second, utilities should be prohibited from sharing customer data with third parties unless the third parties agree, as a condition of receiving the data, to abide by specific FIPs principles, including: the full and complete disclosure of all uses of customer data; required reauthorization for changes in use; data breach notification; and privacy audits. The Commission should control downstream use of the data by conditioning access to the data on certain privacy and security requirements, including requiring regulated entities to condition third-party access to customer data on those

third parties agreeing to meet the requirements. The full text of our proposed rule can be found in Appendix A.

A. Before a Utility May Transfer Data to a Third Party, the Third Party Must Disclose Uses to and Obtain Authorization from Customers

To protect consumers' privacy and security, the Commission should require utilities to include customer privacy protections in their contracts and dealings with third parties. First, to avoid unauthorized uses of a customer's data by a third party, third parties should disclose all of the intended uses of customer data before authorization. This disclosure will enable customers to make an informed decision and permit informed consent. Thus, our suggested modifications to the proposed Rule place certain disclosure requirements on third parties that contract with utilities for customer data. It requires third parties to disclose to the customer, prior to the customer's authorization to provide access to the third party: (1) "each specific use of the customer data," (2) "all other parties with whom the entity will share customer data," and (3) "a list of all of the data elements that will be transferred to the entity. . . ."[69] Clearly articulating the purpose of the data use, all parties that will use the data, and the exact data being shared, enables the consumer to make an informed choice before deciding to share data.

Further, the Proposed Rule currently requires utilities to provide authorized third parties with "advanced meter data, including meter data used to calculate charges for electric service, historical load data and any other proprietary customer information. . . ."[70] The default rule should not be full disclosure of all proprietary customer information. Our modified Rule provides that utilities only disclose information "that is necessary to accomplish the uses specifically disclosed to and authorized by the customer."[71] Utilities should review third parties' disclosed uses and should only provide the individual data fields necessary for those disclosed uses.

B. Utilities Should Enforce Third Party Contractual Obligations

Once the utility transfers data to a third party a new set of risks and concerns arise. As described above, customer data is likely to be of interest to a wide variety of parties, for a wide

[69] *See infra* app. A, § 1(a)(i) (Modified Proposed Access Rule).
[70] *Id.* app. A, § 1.
[71] *Id.* app. A, § 1(b).

variety of purposes. Without intervention by the Commission, a third party that obtains customer information could sell that information to other third parties or use it in ways that were not authorized by the customer. The Commission should use its regulatory authority to ensure that any customer information transferred from a utility to a third party is sufficiently protected by requiring third parties to be contractually bound by the utilities as part of the consideration for receipt of customer data.

1. Prohibition On Non-Disclosed Uses and Parties

The Commission should require that utilities include clauses in contracts with third parties that require those third parties, as a condition of receiving customer data, to only use that data only for the specific purposes disclosed to the customer. Similarly, third parties should "not disclose customer data to any entities other than those entities expressly disclosed to and authorized by the customer. . . ."[72] For example, a consumer should not receive unsolicited advertisements based upon energy usage data that her energy efficiency consultant sold to appliance marketers without her authorization. If a third party later wants to use customer data for other uses or provide it to other parties, it must obtain "specific re-authorization, in writing or via electronic signature" for those new uses or other parties.[73]

2. Privacy Impact Assessments

As part of the regular privacy impact audits and assessments we recommend the utilities conduct,[74] the Commission should require all entities in possession of customer data to conduct, and report to the Commission, "independent audit[s] of the security of customer data and entity compliance with its disclosed usage policy. . . ."[75] Such assessments are critical to understanding whether measures to protect privacy are successful or if they create cost without providing sufficient benefit, will guide entities in improving practices, and support the Accountability and Auditing principle.

---

[72] *Id.* app. A, § 1(a)(ii).
[73] *Id.* app. A, § 1(a)(iii).
[74] *See supra* § V.A.8 (Accountability and Auditing).
[75] *See infra* app. A, § 2.

3. Data Quality and Integrity

Customers should have the right to see what data an entity possesses about them and to correct any inaccuracies in that data. The requirement is an important component of the FIPs Data Quality and Integrity principle, discussed in more detail above.[76] Our modified rule would require that entities possessing customer data "provide a means for customers to view their customer data held by the entity, a means to correct data inaccuracies, and a procedure to correct inaccuracies within thirty (30) days' notice of the inaccuracies."[77]

4. Data Destruction

Based upon the FIPs Data Minimization principle,[78] our modified Rule would require entities in possession of customer information to "destroy customer data when it is no longer necessary for the uses disclosed to the customer. . . ."[79] Destroying unnecessary data significantly reduces the risk of unauthorized use and disclosure of customer information.

5. Data Breach Notification

In Section V.C, we urged the Commission to apply California's Data Breach Notification Law, section 1789.29 of the Civil Code, to regulated entities. The Commission should likewise require third parties that handle customer data to notify customers and the Commission of any unauthorized disclosure, use, or access of the customer data, so that the customer can take appropriate steps to protect herself and modify her behavior accordingly (for example, by ceasing to share information with the party that allowed the breach). Requiring third parties to provide notification will provide strong incentives for safe and secure information practices so they can avoid the cost and embarrassment of having to report a data breach. Section 3(c) of our proposed Rule thus requires any entity in possession of proprietary customer information to follow the section 1789.29 data breach notification rules.

---

[76] *See supra* § V.A.6 (Data Quality and Integrity).
[77] *Id.* app. A, § 3(a).
[78] *See supra* §V.A.4 (Data Minimization).
[79] *See infra* app. A, § 3(b).

C. Other Third Party Access Rules That the Commission Should Consider

1. Government Access to Customer Information

We urge the Commission to specify, within the Proposed Access Rule, when and how utilities should provide customer information to law enforcement officials and other government agencies. Under both California and Federal law, the home, as a retreat from the outside world and from the government, is an especially protected space, with an especially strong privacy interest attached to it.

Longstanding United States constitutional values and precedent afford special protection for activities occurring within the sanctity of individuals' homes because of their inherently personal nature. The Fourth Amendment draws "a firm line at the entrance to the house,"[80] because "privacy expectations are most heightened" in the "private home."[81] The Supreme Court affirmed this protection for all types of data found in the home, noting in *Kyllo v. United States* that the "Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained. . . . In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes."[82] In *Kyllo*, the Court invalidated the warrantless use of thermal imaging technology to measure heat emanating from a home as an unlawful search under the Fourth Amendment, despite the lack of any physical intrusion into the home by law enforcement.[83] Data collected via Smart Grid technologies is similarly revealing of the intimate details of home life and should be subject to at least the same high levels of protection that the Supreme Court required of law enforcement in *Kyllo*.

Californian's constitutional privacy protections extend further than general Fourth Amendment protections and have been found to protect business records.[84] Although the California Supreme Court has not yet addressed energy privacy, it has recognized a protected privacy interest in other records held by third parties. For example, in *Burrows v. Superior*

---

[80] *Payton v. New York*, 445 U.S. 573, 590 (1980).
[81] *Dow Chemical Co. v. United States*, 476 U.S. 227, 237 n.4 (1986); *see Boyd v. United States*, 116 U.S. 616, 630 (1886) ("It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property[.]").
[82] *Kyllo v. United States*, 533 U.S. 27, 37 (2001).
[83] *Id.* at 40.
[84] *See, e.g., Valley Bank of Nev. v. Superior Court*, 15 Cal. 3d 652 (1975).

Court,[85] the court held that customer information voluntarily disclosed by a bank to law enforcement officers without the customer's knowledge or consent was the product of an unlawful search and seizure under article I, section 13, of the California Constitution. The court went on to hold that customers expect that the information they share with their banks will remain private, and that "absent compulsion by legal process . . . [the customer expects the matters he] reveals to the bank will be utilized by the bank only for internal banking purposes."[86] Later cases have similarly protected telephone records.[87]

Article 1, section 1 of the California Constitution provides additional protections. In *Brillantes v. Superior Court*, the court held that "an intrusion upon constitutionally protected areas of privacy requires a balancing of the juxtaposed rights, and the finding of a compelling state interest."[88] The court allowed the seizure of medical records only where "the state [had] demonstrated a compelling interest in the medical records related to the Medi-Cal fraud investigation."[89] Similarly, in *McKirdy v. Superior Court*, the court affirmed "any [incursion into individual privacy] must be justified by a compelling interest."[90]

The Commission has already recognized that the privacy protections inherent in sections 1 and 13 of article 1 of the California Constitution extend to cover customer energy data. In Decision No. 90-12-121 and its appeal, Decision No. 01-07-032, the Commission extensively examined privacy concerns related to law enforcement access to utility data and, relying on the *Burrows*,[91] *Blair*,[92] and *Chapman*[93] line of cases, determined that it should not be disclosed to law enforcement without adequate legal process.[94] We urge the Commission to follow this precedent and re-affirm that law enforcement and government agencies must obtain adequate legal process before accessing customer energy usage data. Because of the unusually private nature of granular energy usage data, we urge the Commission to go a step further and require law enforcement to show probable cause in the form of a warrant before a utility releases such

---

[85] 13 Cal. 3d 238 (1974).
[86] *Id.*
[87] *People v. Blair*, 25 Cal. 3d 640, 653-54 (1979); *People v. Chapman*, 36 Cal. 3d 98 (1984).
[88] 51 Cal. App. 4th 323, 340 (1996).
[89] *Id.* at 342.
[90] 138 Cal. App. 3d 12, 22 (1996).
[91] 13 Cal. 3d 238.
[92] 25 Cal. 3d 640.
[93] 36 Cal. 3d 98.
[94] D.90-12-121; D.01-07-032.

data. Providing such data to law enforcement without a warrant would be inconsistent with Californians' constitutional right to privacy[95] and the federal Constitution.

2. Civil Litigant Access to Customer Information

In the context of civil litigation, given the sensitivity of smart meter data and its potential to reveal private details of home life, there should be a preference for seeking such data not from the utility, but from the customer directly (who, under our recommendations, should have access to data pertaining to his or her home energy usage). If the only way a civil litigant can obtain the information is directly from a regulable entity, then the litigant should be required to show a compelling interest in the information.

In *White v. Davis*,[96] the first California Supreme Court case to interpret article 1, section 1, of the state constitution, the Court solidified Californian's right to informational privacy. The court held that the constitutional privacy right protects citizens from use of personal information "for another purpose or the disclosure of it to some third party."[97] The court later held in *Hill v. National Collegiate Athletic Assn.*,[98] and affirmed in *American Academy of Pediatrics v. Lungren*,[99] that in cases where there is an obvious invasion of a right fundamental to informational privacy or autonomy, a "compelling interest must be present to overcome the vital privacy interest."[100] If, in contrast, the privacy interest is less central, or in bona fide dispute, a general balancing test is employed.[101] Because of the intrusive nature of energy usage data, as described above, civil litigants should be required to show a compelling interest in the information.

Further, California case law has held that entities receiving subpoenas for private information on their customers must notify the customers prior to disclosing the information and allow time for them to respond. The Commission should similarly protected customer energy information. In *Valley Bank of Nevada v. Superior Court,* the California Supreme Court held that "before confidential customer information may be disclosed in the course of civil discovery

---

[95] Cal. Const. art. 1, §§ 1, 13.
[96] 13 Cal 3d 757 (1974).
[97] *Id.* at 775.
[98], *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1 (1994).
[99] *Am. Academy of Pediatrics v. Lungren,* 16 Cal. 4th 307 (1997).
[100] *Hill*, 7 Cal. 4th at 34.
[101] *Id.*

proceedings, [a] bank must take reasonable steps to notify its customer."[102] Similarly, in *Sehlmeyer v. Department of General Services*, the court held that the constitutional right to privacy requires "that an administrative subpoena duces tecum [seeking a third party witness's medical records] must be preceded by notice to the witness."[103] The courts have also recognized the need to "afford the third party a fair opportunity to assert her interests by objecting to disclosure, by seeking an appropriate protective order[,] or by instituting other legal proceedings to limit the scope or nature of [discovery]."[104]

To keep utility practices in line with California case law, the Commission should require that utilities and other regulated entities only disclose customer data to civil litigants upon being provided with a court order based on a showing of compelling interest and after notifying the customer to provide her with a chance to object.

3. Rules Regarding Third-Party Handling of Customer Information Received Directly from Consumers

The discussion above urges the Commission to adopt rules regulating the use of customer information by utilities and third parties to whom utilities provide customer data. These suggestions are in response to the Commission's specific questions regarding these entities. However, numerous other third parties presently obtain, or plan to obtain, energy usage data directly from the consumer via devices installed in the home, below the meter. For example, Google's' "Power Meter" device captures energy usage data directly from consumers, below the meter. Google presently does not charge for the service.[105] In these situations, the utilities may not be able to act as a gatekeeper for the information. The customer data obtained by these third parties is no less private than the customer data collected and transferred by the utilities, nor would its misuse be any less invasive. As such, we urge the Commission and other regulators to adopt rules similar to the ones outlined here[106] for all parties collecting, using, and transmitting customer information, whether they obtain that data above or below the meter.

---

[102] 15 Cal. 3d 652, 658 (1975).
[103] 17 Cal. App. 4th 1072, 1079 (1993).
[104] *Id.* at 1085 (citing *Valley Bank of Nev. v. Superior Court*, 15 Cal. 3d 652, 658 (1975)).
[105] For information on Google's service, see Google Power Meter, Frequently Asked Questions, http://www.google.org/powermeter/faqs.html (last visited Mar. 9, 2010).
[106] *See supra* §§ VII.A, B; *see also infra*, app. A.

VIII. The Commission Should Include Privacy-Related Quantitative Metrics for Smart Grid Implementations

We support the Commission's proposed use of metrics as a measure of Smart Grid deployment and strongly support the specific use of privacy metrics as a means of measuring the privacy vulnerabilities of the deployed Smart Grid. We recommend that such metrics should be required components of all Smart Grid deployment plans and should be updated by regulated utilities in subsequent proceedings relating to discrete Smart Grid implementations and ratemakings. We propose the following additions and modifications to the Commission's proposed metrics in Attachment C of the Joint Ruling, based on our identification of privacy risks in Section II.B and discussion of Fair Information Practice principles in Section V above.

A. Cyber Security Metrics

The Commission should add the following metrics to Section 2 of the Proposed Metrics to fill the placeholder for cyber security metrics:

- Number of security breaches experienced by the utility or third parties to which the utility provides customer information.
- Number and percentage of customers affected by the security breaches.
- Number and percentage of customer records accessed during the security breaches.
- Average number of days between the security breach and when the customers are notified.
- Number of attempted cyber attacks on the utility or third parties to which the utility provides customer information.
- Monetary damages suffered by utilities or consumers as a result of cyber attacks on the utility or its infrastructure.
- Amount of annual operational expenditure on cyber security.
- Percentage of expenditure on cyber security in the overall operating expense.

- Amount of damages incurred to customers' smart devices as a result of cyber attacks.

- Number of security and privacy impact assessments performed by utilities.

B. Privacy Metrics

We also recommend the following modifications and additions to the proposed metrics in Attachment C of the Joint Ruling to prevent additional privacy harms and to give the Commission specific insight into consumer privacy protections:

- Remove the first item under Section 5 which presently reads "the number and percentage of electricity customers . . . served by appliances and/or equipment which can communicate information automatically about on/off status and availability for load control." This proposed metric encourages the use of customer devices to reveal detailed status information to the utility. This metric is adverse to the privacy interest of residential customers and should be removed.

- Allowing customers to control the granularity of data flowing outside their homes is crucial to privacy. Therefore, we recommend adding the following metrics to Section 9 "Provide Consumers with Timely Information and Control Options:"
    - Number of customers able to control the time interval of smart meter reading reported to utility.
    - Number of customers that exercise control over the time interval of smart meter reading reported to utility.
    - Number of customers able to control their smart devices with their own Energy Management System.
    - Number of customers that exercise control over their smart devices with their own Energy Management System.

- Customer concern about privacy represents a barrier to Smart Grid adoption. Therefore, we recommend adding the following metrics to Section 11 "Lowering Barriers to Adoption of Smart Grid:"
    - Amount of customer information collected about an average residential customer and retention period of such data.
    - Number and type of third party entities receiving customer information under the [Proposed] Access Rule.
    - Number and type of law enforcement or other government requests to access customer information held by the utility or the third parties to whom the utility provides information, and the compliance with such requests.
    - Number of individuals whose customer information was provided to law enforcement or other government agencies.
    - Number and type requests by civil litigants to access customer information held by the utility and the compliance with such requests.
    - Number and type of third parties to whom the utility provides information, and the compliance with such requests.
    - Number and type of data breach notifications during the reporting period.

Finally, the Commission should delete the first metric in Section 6 of the Proposed Metrics: "Number of consumer devices actively communicating with Home Area Networks." This metric is detrimental to data minimization and therefore to privacy protection, as it requires utilities to obtain information about appliances within consumers' homes. A consumer may have deployed a Home Area Network for the express purpose of protecting her privacy by hiding the devices within the home from the utility. Such metrics, relating to in-home deployment, should take into account the fact that privacy-friendly smart devices may be invisible to the utilities. The Commission's metrics should respect customers' desire for privacy and not encourage the utilities to collect detailed device information from residential customers.

IX. The Commission Should Not Wait for Privacy Standards from the National Standard-Setting Bodies, and Should Adopt Fair Information Practice Principles Now

State Senate Bill 17 instructs the Commission to "adopt standards and protocols to ensure functionality and interoperability developed by public and private entities, including, but not limited to, the National Institute of Standards and Technology, Gridwise Architecture Council, the International Electrical and Electronics Engineers, and the National Electric Reliability Organization recognized by the Federal Energy Regulatory Commission."[107] As the Commission has observed, however, the national standard-setting organizations have not yet released final drafts of their standards and protocols.[108] The Commission seeks comment on three possible approaches to this problem.

1) Deferring Commission consideration in this proceeding until a number of the listed agencies have adopted standards or protocols;

2) Deferring Commission consideration of protocols to another proceeding that will commence after a number of the listed agencies have adopted standards or protocols; or

3) Adopting a "performance standard" in this proceeding requiring that those implementing a Smart Grid technology take steps to ensure that it has the capability to function and operate with devices developed pursuant to standards adopted by major standard setting agencies.[109]

In light of the rapid deployment of Smart Grid technologies already underway in California, approaches (1) and (2) above appear as problematically slow for addressing adequately issues of privacy and consumer protection. It is unclear how long it will take for "a number of the listed agencies" to adopt standards; smart devices deployed during this open-ended time period, risk non-compliance with both the technical standards and privacy standards that the Commission eventually adopts.

At the same time, approach (3) appears not to address privacy issues, at all, as the

---

[107] Cal. Pub. Util. Code § 8362.
[108] Feb. Joint Ruling, *supra* note 39, at 19.
[109] *See id.* These three options are slightly reworded from the language in the original ruling.

"functional operability with other devices" requirement carries no privacy protections or restrictions. Further, approach (3) shifts significant standards decision-making authority to the utilities themselves, creating a self-regulatory regime and depriving the utilities of meaningful Commission guidance on relevant standards. For this reason, it is unclear whether approach 3 succeeds in meeting the obligations imposed by SB 17.

We thus urge the Commission to pursue a fourth option, at least with regard to privacy requirements. The Commission should adopt concrete privacy requirements based on the Fair Information Practice principles without delay, and should compare technical and other standards presented to it against these requirements. If national standards or guidelines related to privacy protections are promulgated in the future, the Commission can open a new proceeding to consider these.

As described further above in Section V,[110] the FIPs are a widely recognized and well established framework for information management. Indeed, it is unlikely that any of the national standard-setting organizations would release privacy standards that were not reflective of, or influenced by, the Fair Information Practice principles. If the Commission later considers adoption of standards from these national standard-setting organizations, we urge the Commission to disregard outright any set of standards that does not reflect the FIPs framework.

Privacy is a valued constitutional right in California, and the Commission has adequate authority, under article 1, section 1 of the California Constitution to adopt Smart Grid privacy standards immediately and on its own initiative,[111] independent of authority granted it by SB 17. We urge that the Commission adopt the Fair Information Practice principles as California's Smart Grid privacy protection framework. California also has a strong history of being at the forefront of both environmental and privacy regulation. Where California leads, the rest of the states and the federal government follow. The Smart Grid provides the Commission with an opportunity to help California to continue to lead the country in environmental regulation and privacy protection.

[110] For a comprehensive overview and explanation of the FIPs, please refer to § V, *supra*.
[111] *See* discussion *supra* § III.

X. Conclusion

The Center for Democracy & Technology and the Electronic Frontier Foundation appreciate the opportunity to submit these comments in response to the Assigned Commissioner and Administrative Law Judge's Joint Ruling Inviting Comments on Proposed Policies and Findings Pertaining to the Smart Grid, issued February 8, 2010. We commend the Commission on its careful consideration of the consumer privacy risks presented by the emerging Smart Grid, and we thank the Commission again for its consideration of the privacy recommendations we have presented here.

Respectfully submitted this March 9, 2010 at San Francisco, California.

/s/ Jennifer Lynch

JENNIFER LYNCH, Attorney
Samuelson Law, Technology & Public Policy Clinic
University of California, Berkeley School of Law
396 Simon Hall
Berkeley, CA 94720-7200
(510) 642-7515
Attorney for CENTER FOR DEMOCRACY & TECHNOLOGY

/s/ Lee Tien

LEE TIEN, Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333 x102
Attorney for ELECTRONIC FRONTIER FOUNDATION

APPENDIX A – Modifications to Language of Proposed Third Party Access Rules[112]

1. An electrical corporation shall provide a customer, the customer's electric service provider (ESP), the customer's demand response provider (DRP), or other third party entity authorized by the customer read-only access to the customer's advanced meter data, including meter data used to calculate charges for electric service, historical load data and any other proprietary customer information (collectively, "customer data") only as described herein in sections 1 through 8. ESPs, DRPs, or any other third parties that obtain customer data shall not disclose or use that customer data except as described herein in sections 1 through 8. The access shall be convenient and secure, and the data shall be made available no later than the next day of service. Such authorization may be made in writing or via electronic signature, consistent with industry, privacy and security standards and methods. The utility may only transfer customer data:

    a. to an entity that is either (i) already bound by this section or (ii) contractually agrees, in consideration of receiving the data, to

        i. fully disclose to the customer, prior to obtaining authorization:

            1. each specific use of the customer data,

            2. all other parties with whom the entity will share the customer data, and

            3. a list of all of the data elements that will be transferred to the entity (these may include, for example, name, address, social security number, meter readings [including the frequency of measurements being provided], appliance ID numbers, or any other discrete types of information being transferred);

[112] Throughout this Appendix A, we have used specific formatting to denote changes. The proposed additions that the Commission denoted in its Feb. Joint Ruling with underlined text have been included in our Appendix text without an underline. We have illustrated our further additions with an underline. Text that is formatted with a strikethrough *only* represents the text in the Feb. Joint Ruling that was also presented in strikethrough. Text that is contains both an *underline and a strikethrough* is text that was provided in the Feb. Joint Ruling and that we recommend omitting.

ii. not disclose customer data to any entities other than those entities expressly disclosed to and authorized by the customer under (i), above;

iii. obtain separate, specific re-authorization, in writing or via electronic signature, for any new use of customer data or new entity with which it plans to share the data, consistent with (i), above; and

iv. abide by the regulations in sections 2 and 3, below; and

b. that is necessary to accomplish the uses specifically disclosed to and authorized by the customer.

2. An electrical corporation or other entity providing customer data shall use at a minimum industry standards and methods for providing secure customer, ESP, DRP and third party access to a specified customer's ~~meter~~ data. For purposes of these Rules, "industry standards" shall include those industries that routinely deal with highly personal, sensitive and confidential information, including but not limited to the financial industry and the medical information industry. ~~[The electrical corporation~~ All entities in possession of customer data shall have an independent security audit of the mechanism for customer and third party access to ~~meter~~ customer data conducted within one year of initiating such access and report the findings to the Commission.~~]~~ Thereafter, all entities in possession of customer data shall have an independent audit of the security of customer data and entity compliance with its disclosed usage policy on an annual basis and shall report the findings to the Commission, which shall make the reports publicly available.

3. All entities in possession of customer data shall:

a. provide a means for customers to view their customer data held by the entity, a means to correct data inaccuracies, and a procedure to correct inaccuracies within thirty (30) days' notice of the inaccuracies;

b. destroy customer data when it is no longer necessary for the uses disclosed to the customer;

c. follow the data breach notification rules described in Cal. Civ. Code § 1798.29, for the loss or unauthorized acquisition of or access to customer data; and,

d. only disclose customer data to law enforcement after being provided with a warrant.

e. only disclose customer data to civil litigants after being provided with a court order based on a showing of compelling interest and after notifying the customer to provide the customer with a chance to object to disclosure.

4. ~~3.~~ The California Independent System Operator, or any subsequent regional transmission organization or regional reliability entity, shall have access only to information necessary or required for wholesale settlement, load profiling, load research and reliability purposes.

5. ~~4.~~ A customer may authorize, either in writing or by electronic signature, its customer data to be available to an entity other than its Load Serving Entity or Utility Distribution Company, subject to the requirements of sections 1 through 3.

6. ~~5.~~ An electrical corporation shall provide access to data, as described above, in a manner consistent with and in accordance with the time frame as decided by the Commission in Decision _____,

Revised rule modeled on Tariff Rule 22[56]

7. ~~3.~~ Providing Access to Customer Data Captured by AMI for Authorized Third Parties

[Insert utility] will only provide customer-specific usage data to parties specified and authorized by the customer, subject to the provisions in sections 1 through 3 above, and the following provisions:

a. ~~Except as provided in Section d, t~~The inquiring party must have ~~written~~ authorization from the customer, either in writing or by electronic signature, to release such

[56] Tariff Rule 22 was the tariff adopted by electric utilities to provide for Direct Access Service. A copy of PG&E's Tariff Rule 22 is available online at: external link: http://beta1.pge.com/nots/rates/tariffs/pdf/ER22.pdf. The relevant portion is at C.3, on tariff sheets 11-12.

information to the inquiring party only. Such authorization must be revocable. At the customer's request, this authorization may also indicate if customer information may be released to other parties as ~~specified~~ specified and authorized by the customer.

b. Subject to customer authorization, [~~I~~insert utility] will provide ~~a maximum of~~ not more than the most recent twelve (12) months of customer usage data ~~or the amount of data for that specific service account~~ in a format consistent with industry standards, including privacy and security standards, as approved by the Commission. Customer information will be released to the customer or an authorized agent ~~up to two (2) times per year per service account~~ at no cost to the ~~requesting party~~ or the customer. ~~Thereafter, [insert utility] will have the ability to assess a processing charge only if approved by the Commission.~~

c. ~~As a one time requirement at the initiation of Direct Access,~~ [~~i~~Insert utility] will make available a database containing a twelve (12) month history of customer-specific customer's data usage information with geographic and SIC information, but with customer identities removed, to a ~~customer's ESP, DRP or other~~ third party~~ies~~ approved by the Commission, subject to the requirements of this provision and provisions 1 through 3, and only where a customer has authorized such disclosure. ~~[Insert utility] will have the ability to assess a charge only if approved by the Commission.~~

~~d. By electing to take Direct Access service from an ESP, the customer consents to release to the ESP metering information required for billing, settlement and other functions required for the ESP to meet its requirements and twelve (12) months of historical data.~~

d. A third party receiving customer data pursuant to this section shall use such data only for the purposes to which the consumer consented and shall be subject to the same rules on privacy and security that are applicable to utilities handling customer data.

~~d. By authorizing third party to access their information, the customer consents to release to a third party information required for billing, settlement and other functions~~

~~and services required for that entity to meet its requirements and obligations and twelve (12) months of historical data.~~

CERTIFICATE OF SERVICE

I hereby certify that, pursuant to the Commission's Rules of Practice and Procedure, I have this day served a true copy of this document, JOINT COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY AND THE ELECTRONIC FRONTIER FOUNDATION ON PROPOSED POLICIES AND FINDINGS PERTAINING TO THE SMART GRID, on all parties identified on the attached official service list for Proceeding: R08-12-009. Service was completed by serving an electronic copy on their email address of record and by mailing paper copies to parties without email addresses.

Executed on March 9, 2010 at Berkeley, California

/s/ Jennifer Lynch
JENNIFER LYNCH, Attorney
Samuelson Law, Technology & Public Policy Clinic
University of California – Berkeley School of Law
396 Simon Hall
Berkeley, CA 94720-7200

SERVICE LIST

carlgustin@groundedpower.com
jeffrcam@cisco.com
cbrooks@tendrilinc.com
npedersen@hanmor.com
slins@ci.glendale.ca.us
douglass@energyattorney.com
ffletcher@ci.burbank.ca.us
kris.vyas@sce.com
atrial@sempra.com
lburdick@higgslaw.com
liddell@energyattorney.com
mshames@ucan.org
ctoca@utility-savings.com
bobsmithttl@gmail.com
mtierney-lloyd@enernoc.com
ed@megawattsf.com
mterrell@google.com
mdjoseph@adamsbroadwell.com
pickering@energyhub.net
margarita.gutierrez@sfgov.org
lms@cpuc.ca.gov
fsmith@sfwater.org
srovetti@sfwater.org
tburke@sfwater.org
lettenson@nrdc.org
marcel@turn.org
mkurtovich@chevron.com
SSchedler@foe.org
cjw5@pge.com
nes@a-klaw.com
pcasciato@sbcglobal.net
steven@sfpower.org
mgo@goodinmacbride.com
mday@goodinmacbride.com
ssmyers@worldnet.att.net
lex@consumercal.org
farrokh.albuyeh@oati.net
Service@spurr.org
wbooth@booth-law.com
jwiedman@keyesandfox.com
kfox@keyesandfox.com
enriqueg@greenlining.org
gmorris@emf.net
kerry.hattevik@nrgenergy.com
rquattrini@energyconnectinc.com
seboyd@tid.org
martinhomec@gmail.com
dzlotlow@caiso.com
dennis@ddecuir.com
scott.tomashefsky@ncpa.com
jhawley@technet.org
lnavarro@edf.org
Lesla@calcable.org
cbk@eslawfirm.com
gstaples@mendotagroup.net
jlin@strategen.com
MNelson@MccarthyLaw.com
EGrizard@deweysquare.com
Mike.Ahmadi@Granitekey.com
r.raushenbush@comcast.net
tam.hunt@gmail.com
john.quealy@canaccordadams.com
mark.sigal@canaccordadams.com
barbalex@ctel.net
crjohnson@lge.com
julien.dumoulin-smith@ubs.com
david.rubin@troutmansanders.com
jennsanf@cisco.com
marybrow@cisco.com
jmccarthy@ctia.org
jay.birnbaum@currentgroup.com
bboyd@aclaratech.com
bob.rowe@northwestern.com
monica.merino@comed.com
sthiel@us.ibm.com
ed.may@itron.com
rgifford@wbklaw.com
leilani.johnson@ladwp.com
dschneider@lumesource.com
david@nemtzow.com
cjuennen@ci.glendale.us
fhall@solarelectricsolutions.com
mark.s.martinez@sce.com
case.admin@sce.com
michael.backstrom@sce.com
nquan@gswater.com
Jcox@fce.com
esther.northrup@cox.com

kfoley@sempra.com
kmkiener@cox.net
ygross@sempra.com
rwinthrop@pilotpowergroup.com
CentralFiles@semprautilities.com
tcahill@semprautilities.com
cmanson@semprautilities.com
jerry@enernex.com
traceydrabant@bves.com
peter.pearson@bves.com
dkolk@compenergy.com
ek@a-klaw.com
rboland@e-radioinc.com
sue.mara@rtoadvisors.com
juan.otero@trilliantinc.com
mozhi.habibi@ventyx.com
faramarz@ieee.org
elaine.duncan@verizon.com
mandywallace@gmail.com
norman.furuta@navy.mil
kgrenfell@nrdc.org
mcarboy@signalhill.com
nsuetake@turn.org
bfinkelstein@turn.org
andrew_meiman@newcomb.cc
ayl5@pge.com
DNG6@pge.com
fsc2@pge.com
filings@a-klaw.com
Kcj5@pge.com
mpa@a-klaw.com
rcounihan@enernoc.com
stephen.j.callahan@us.ibm.com
tmfry@nexant.com
bcragg@goodinmacbride.com
bdille@jmpsecurities.com
cassandra.sweet@dowjones.com
jscancarelli@crowell.com
jas@cpdb.com
nml@cpdb.com
SDHilton@stoel.com
Diane.Fellman@nrgenergy.com
cem@newsdata.com
lisa_weinzimer@platts.com
prp1@pge.com
achuang@epri.com
caryn.lai@bingham.com
epetrill@epri.com
ali.ipakchi@oati.com
chris@emeter.com
sharon@emeter.com
ralf1241a@cs.com
sean.beatty@mirant.com
john_gutierrez@cable.comcast.com
t_lewis@pacbell.net
Valerie.Richardson@us.kema.com
nellie.tong@us.kema.com
Douglas.Garrett@cox.com
rstuart@brightsourceenergy.com
mrw@mrwassoc.com
cpucdockets@keyesandfox.com
dmarcus2@sbcglobal.net
rschmidt@bartlewells.com
jlynch@law.berkeley.edu
jurban@law.berkeley.edu
kco@kingstoncole.com
philm@scdenergy.com
j_peterson@ourhomespaces.com
joe.weiss@realtimeacs.com
michaelboyd@sbcglobal.net
bmcc@mccarthylaw.com
sberlin@mccarthylaw.com
mary.tucker@sanjoseca.gov
tomk@mid.org
joyw@mid.org
brbarkovich@earthlink.net
gayatri@jbsenergy.com
dgrandy@caonsitegen.com
demorse@omsoft.com
martinhomec@gmail.com
e-recipient@caiso.com
hsanders@caiso.com
jgoodin@caiso.com
wamer@kirkwood.com
tpomales@arb.ca.gov
brian.theaker@dynegy.com
danielle@ceert.org
dave@ppallc.com
jmcfarland@treasurer.ca.gov
shears@ceert.org
kellie.smith@sen.ca.gov
lkelly@energy.state.ca.us

mgarcia@arb.ca.gov
ro@calcable.org
steven@lipmanconsulting.com
lmh@eslawfirm.com
abb@eslawfirm.com
bsb@eslawfirm.com
glw@eslawfirm.com
jparks@smud.org
ljimene@smud.org
ttutt@smud.org
vzavatt@smud.org
vwood@smud.org
dan.mooy@ventyx.com
kmills@cfbf.com
rogerl47@aol.com
jellis@resero.com
michael.jung@silverspringnet.com
wmc@a-klaw.com
bschuman@pacific-crest.com
sharon.noell@pgn.com
californiadockets@pacificorp.com
ag2@cpuc.ca.gov
agc@cpuc.ca.gov
am1@cpuc.ca.gov
crv@cpuc.ca.gov
df1@cpuc.ca.gov
dbp@cpuc.ca.gov
trh@cpuc.ca.gov
fxg@cpuc.ca.gov
gtd@cpuc.ca.gov
jw2@cpuc.ca.gov
jdr@cpuc.ca.gov
jmh@cpuc.ca.gov
kar@cpuc.ca.gov
kd1@cpuc.ca.gov
lau@cpuc.ca.gov
zaf@cpuc.ca.gov
mjd@cpuc.ca.gov
mc3@cpuc.ca.gov
wtr@cpuc.ca.gov
rhh@cpuc.ca.gov
srt@cpuc.ca.gov
scl@cpuc.ca.gov
scr@cpuc.ca.gov
tjs@cpuc.ca.gov
vjb@cpuc.ca.gov
wmp@cpuc.ca.gov
BLee@energy.state.ca.us
ab2@cpuc.ca.gov

MARCH 10, 2010 | BY LEE TIEN

New "Smart Meters" for Energy Use Put Privacy at Risk

The ebb and flow of gas and electricity into your home contains surprisingly detailed information about your daily life. Energy usage data, measured moment by moment, allows the reconstruction of a household's activities: when people wake up, when they come home, when they go on vacation, and maybe even when they take a hot bath.

California's PG&E is currently in the process of installing "smart meters" that will collect this moment by moment data—750 to 3000 data points per month per household—for every energy customer in the state. These meters are aimed at helping consumers monitor and control their energy usage, but right now, the program lacks critical privacy protections.

That's why EFF and other privacy groups filed comments with the California Public Utilities Commission Tuesday, asking for the adoption of strong rules to protect the privacy and security of customers' energy-usage information. Without strong protections, this information can and will be repurposed by interested parties. It's not hard to imagine a divorce lawyer subpoenaing this information, an insurance company interpreting the data in a way that allows it to penalize customers, or criminals intercepting the information to plan a burglary. Marketing companies will also desperately want to access this data to get new intimate new insights into your family's day-to-day routine-not to mention the government, which wants to mine the data for law enforcement and other purposes.

This isn't just a California issue. Many threats to the privacy of the home—where our privacy rights should be strongest—were detailed in a 2009 report for the Colorado Public Utility Commission. The federal government has been promoting the smart grid as part of its economic stimulus package, and last year, EFF and other groups warned the National Institute of Standards and Technology about the privacy and security issues at stake. For example, security researchers worry that today's smart meters and their communications networks are vulnerable to a variety of attacks. There are also questions of reliability, as PG&E faces criticism from California customers who have seen bills skyrocket after the installation of the new "smart meters." Unsurprisingly, California legislators are questioning the rapid rollout. Texas customers are also complaining.

There are far more questions than answers when it comes to this new technology. While it's potentially beneficial, it could also usher in new intrusions into our home and private life. The states and the federal government should ensure that energy customers get the protection they deserve.

Special thanks to Berkeley Law students Jonas Herrell, David Marty, and Shane Witnov, along with School of Information Masters Candidate, Longhao Wang for their work in drafting these comments to the California PUC.

Privacy

MORE DEEPLINKS POSTS LIKE THIS

APRIL 2007
Watch Mark Cuban Debate EFF's Fred von Lohmann About YouTube and the Future of Copyright

APRIL 2010
Consumers International Video: When Copyright Goes Bad

APRIL 2007
Proposed Bill Aims to Save Music Webcasters

APRIL 2007
Washington Rejects REAL ID

APRIL 2007
OPEN Government Act Heads to Senate Floor

RECENT DEEPLINKS POSTS

AUG 2, 2013
Prominent Security Researchers, Academics, and Lawyers Demand Congress Reform the CFAA and Support Aaron's Law

AUG 2, 2013
EFF Welcomes New Senior Staff Attorney David Greene

AUG 2, 2013
Encryption is Key: T-Shirt and Puzzle at DEF CON 21

AUG 1, 2013
Oakland's Creepy New Surveillance Program Just Got Approved

AUG 1, 2013
Not-Quite-Open Wireless: What Does it Mean to Be Really Open?

DEEPLINKS TOPICS

Analog Hole
Anonymity
Anti-Counterfeiting Trade Agreement
Biometrics
Bloggers Under Fire
Bloggers' Rights
Broadcast Flag
Broadcast Flag
Broadcasting Treaty
CALEA
Cell Tracking
Coders' Rights Project
Computer Fraud And Abuse Act Reform
Content Blocking
Copyright Trolls
Council of Europe
Cyber Security Legislation
CyberSLAPP
Development Agenda
Digital Books
Digital Radio
Digital Video
DMCA
DMCA Rulemaking
Do Not Track
DRM
E-Voting Rights
EFF Europe
Encrypting the Web
Export Controls
FAQs for Lodsys Targets
File Sharing
Free Speech
FTAA
Hollywood v. DVD
How Patents Hinder Innovation (Graphic)
Innovation
Intellectual Property
International
International Privacy Standards
Internet Governance Forum
Legislative Solutions for Patent Reform
Locational Privacy
Mandatory Data Retention
Mandatory National IDs and Biometric Databases
Mass Surveillance Technologies
National Security Letters
Net Neutrality
No Downtime for Free Speech
NSA Spying
OECD
Online Behavioral Tracking
Open Access
Open Wireless
PATRIOT Act
Pen Trap
Policy Analysis
Printers
Privacy
Reading Accessibility
Real ID
RFID
Search Engines
Search Incident to Arrest
Section 230 of the Communications Decency Act
Security
Social Networks
SOPA/PIPA: Internet Blacklist Legislation
State Surveillance & Human Rights
State-Sponsored Malware
Surveillance Drones
Terms Of (Ab)Use
Test Your ISP
The "Six Strikes" Copyright Surveillance Machine
The Global Network Initiative
Trans Pacific Partnership Agreement
Transparency
Travel Screening
Trusted Computing
Uncategorized

Projects

Bloggers' Rights
Coders' Rights
Follow EFF
Free Speech Weak Links
Global Chokepoints
HTTPS Everywhere
Open Wireless Movement
Patent Busting
Surveillance Self-Defense
Takedown Hall of Shame
Teaching Copyright
Transparency Project
Ways To Help